

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division

UNITED STATES OF AMERICA

v.

Criminal No. 3:19cr19  
UNDER SEAL

TROY GEORGE SKINNER,

Defendant.

**MEMORANDUM OPINION I**  
**The Motion to Suppress Decision**

This matter comes before the Court on six motions brought by Defendant Troy George Skinner. Skinner, a New Zealand citizen, faces kidnapping and production of child pornography charges in the United States.

This opinion addresses Skinner's Motion to Suppress under the Fourth Amendment to the United States Constitution, (the "Motion to Suppress"). (ECF No. 70.) In the Motion to Suppress, Skinner seeks to exclude the fruits of three warrants: one that authorized the search of two cell phones and two warrants that, later, authorized the search of one Google Mail ("Gmail") account each. The United States filed a response in opposition, (ECF No. 80), and Skinner replied, (ECF No. 92). After two evidentiary hearings and additional briefing, the matter is ripe for disposition. For the reasons that follow, the Court will deny the Motion to Suppress.

**I. Procedural History and Findings of Fact**

**A. Procedural History**

On September 18, 2019, a federal grand jury returned an eleven-count superseding indictment (the "Superseding Indictment") against Skinner. (ECF No. 58.) The Superseding Indictment charged Skinner with nine counts relating to the production of child pornography

(Counts 1–9, the “Child Pornography Charges”) and two counts of attempted kidnapping (Counts 10–11, the “Kidnapping Charges”). Four months later, on January 10, 2020, Skinner filed the Motion to Suppress. (ECF No. 70.)

**1. The Motion to Suppress**

The Motion to Suppress relates to three warrants. The first warrant, issued July 20, 2018, authorized the search of two cell phones, a Samsung GT and a Huawei ALE-L02, belonging to Skinner and found near him at time of his arrest (the “Cell Phones Warrant”).<sup>1</sup> The second warrant, issued October 12, 2018, authorized the search of a Gmail account linked to Skinner (the “Johnvlogchamber Gmail Warrant”).<sup>2</sup> The third warrant, also issued October 12, 2018, authorized the search of another Gmail account linked to Skinner (the “Lottic.yzw Gmail Warrant,” and together, “the Gmail Warrants”).<sup>3</sup>

In the Motion to Suppress, Skinner seeks suppression of evidence found on his cell phones and in his Gmail accounts claiming that the search and seizure of them violated his rights under the Fourth Amendment. Specifically, Skinner contends that the Cell Phones and Gmail Warrants were “essentially general warrants” that lacked particularity and did not “establish probable cause sufficient to authorize a wholesale search for all information on the phone or in the accounts.” (Mot. Suppress 2, ECF No. 70.) Skinner argues that the breadth of items covered in the warrants was unconstitutional, as was the manner in which the information was electronically seized. (*Id.* 8–9.) Skinner contends that “the extended [twenty-nine day] seizure

---

<sup>1</sup> For ease of reference, information about the Cell Phones Warrant can be found on the CM/ECF docket at case number 3:18sw180.

<sup>2</sup> For ease of reference, information about the Johnvlogchamber Gmail Warrant can be found on the CM/ECF docket at case number 3:18sw267.

<sup>3</sup> For ease of reference, information about the Lottic.yzw Gmail Warrant can be found on the CM/ECF docket at case number 3:18sw268.

of . . . Skinner's cell phone before obtaining the search warrant was unreasonable." (*Id.* 9 (bold omitted).)

After initial briefing on the Motion to Suppress, (ECFs No. 70, 89, 92), the Court held its First Evidentiary Hearing on February 13, 2020. Following the First Evidentiary Hearing, the Court ordered the United States to file a sur-reply addressing Skinner's argument that the Court could not consider the affidavits attached to the warrants at issue, (Jan. 31, 2020 Order 1, ECF No. 93), which the United States timely submitted, (ECF No. 95). Also at the Court's request, the United States and Skinner filed cross supplemental briefs regarding the Motion to Suppress about arguments raised during the First Evidentiary Hearing, (ECF Nos. 101, 102), and cross-responses, (ECF Nos. 103, 106).

Oral argument was scheduled for March 18, 2020. (ECF No. 107.) As the COVID-19 pandemic took hold, Chief United States District Judge Mark S. Davis entered a General Order continuing all Eastern District of Virginia hearings until after May 1, 2020 for all matters, including the remaining motions here. (Gen. Order 2020-07 (Case No. 2:20mc7), ECF No. 7.) Given these circumstances, on March 13, 2020, the court continued the oral argument with the consent of both parties. (ECF No. 107.) At the Court's direction, the parties jointly submitted a status update citing the General Order and the COVID-19 pandemic and sought a hearing on the pending pretrial motions until sometime after June 1, 2020. (ECF No. 108.) The Court set oral argument for June 12, 2020. That hearing was continued to August 6, 2020, in order to serve the ends of justice, pursuant to General Orders 2020-03, 2020-06, 2020-07, 2020-12, 2020-15, and 2020-16, and accounting for the parties' schedules. (ECF No. 109.)

## 2. The Five Additional Motions

In addition to the Motion to Suppress, Skinner sought to challenge, via five other motions, evidence seized. After the United States and Skinner sought additional time to explore related issues of law,<sup>4</sup> Skinner filed the following additional motions:

- (1) Skinner's Motion to Dismiss Counts One through Nine of the Superseding Indictment for Lack of Subject Matter Jurisdiction and Violation of Due Process (the "Motion to Dismiss for Lack of Subject Matter Jurisdiction"), (ECF No. 69);
- (2) Skinner's Motion to Dismiss Counts One through Nine of the Superseding Indictment on First Amendment Grounds (the "First Amendment Motion to Dismiss"), (ECF No. 71);
- (3) Skinner's Motion to Dismiss Counts One through Nine of the Superseding Indictment on Fifth Amendment Due Process Grounds (the "Fifth Amendment Motion to Dismiss"), (ECF No. 72);
- (4) Skinner's Motion to Sever, (ECF No. 73); and,
- (5) Skinner's Motion for a Jury Questionnaire, (ECF No. 76).

During the August 6, 2020 Second Evidentiary Hearing, the Parties placed evidence on the record<sup>5</sup>—including that produced through the warrants—and the Court heard argument addressing all matters the Parties chose to address orally.

The Court addresses here the Motion to Suppress.<sup>6</sup> Skinner challenges the wholesale search of the contents of his phone and email accounts. At base, Skinner challenges the nature of

---

<sup>4</sup> Skinner initially evaluated whether he would challenge the admissibility of evidence obtained in New Zealand. During the August 6, 2020 oral argument, Counsel for Skinner confirmed they would not challenge the admissibility of evidence seized in New Zealand. (Aug. 6, 2020 Hr'g Tr. 6–7.)

<sup>5</sup> The Parties' stipulation to the evidence may be found on the docket at ECF No. 116.

<sup>6</sup> The Court issues today a second and third opinion. Today's second opinion addresses the Motion to Dismiss for Lack of Subject Matter Jurisdiction, the First Amendment Motion to Dismiss, and the Fifth Amendment Motion to Dismiss, ("Memorandum Opinion II" or "the Constitutional Motions Decision"). The third opinion speaks to the Motion to Sever and the

these electronic searches, contending they lack particularity, probable cause, and were overbroad. (Mot. Suppress 3.) Skinner also contends that “the extended [twenty-nine day] seizure of Skinner’s . . . cell phone before obtaining the search warrant was unreasonable.” (*Id.* 9. (bold omitted).)

**B. Findings of Fact as to the Cell Phones and Gmail Warrants<sup>7</sup>**

On June 22, 2018, officers arrested Skinner, then twenty-four-years old, after he attempted to break into the home of a thirteen-year-old girl, Victim 1 (“V1”), with whom he had had a previous sexual online relationship. When arrested, Skinner possessed two cell phones. The details preceding the arrest, and Skinner’s challenge to the subsequent searches, are articulated below.

---

Motion for a Jury Questionnaire, (“Memorandum Opinion III” or “the Severance Decision”). In each Memorandum Opinion, the Court recounts the facts necessary to resolve the motions at bar.

Skinner raises a different fundamental challenge to the charges brought against him, largely in his Motions to Dismiss, but also here. Skinner argues that no pornography production occurred between him and V1 because all interaction was “virtual.” Because V1 and Skinner never physically touched each other, Skinner argues that these images cannot constitute child pornography.



<sup>7</sup> To promote brevity, the Court makes findings of fact here most pertinent to the Motion to Suppress. The second and third opinions issued today will contain additional facts or procedure most pertinent to the issues addressed there. Because the Court derives its facts from the same two evidentiary hearings and related briefing, the Court incorporates all factual and procedural findings across the three opinions.

**1. The July 20, 2018 Cell Phones Warrant**<sup>8</sup>

On July 20, 2018, Special Agent Melvin Gonzalez of the Federal Bureau of Investigation (“FBI”) applied for a warrant to search two cell phones recovered from Skinner at the time of his arrest. The application was based on an 18-page affidavit (the “Gonzalez Affidavit”) describing potential violations of four criminal statutes, specifically:

- (1) production of child pornography, in violation of 18 U.S.C. § 2251(a);
- (2) distribution or receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2);
- (3) enticement of a minor, in violation of 18 U.S.C. § 2422(b); and,
- (4) kidnapping, in violation of 18 U.S.C. § 1201(a).

(Gonzalez Aff. ¶¶ 7–11).

**2. The Online Communication**

The Gonzalez Affidavit contained sworn testimony that in December 2017, Skinner met on the Internet a thirteen-year-old girl who lived in Goochland, Virginia. The minor (“V1”) told Skinner that she was sixteen years old, although she was only thirteen years old at the time.<sup>9</sup> Skinner truthfully informed V1 that he was twenty-four years old. Skinner and V1 communicated via chat sessions and through livestream video sessions. [REDACTED]

[REDACTED]

---

<sup>8</sup> During the February 13, 2020 Evidentiary Hearing, the Court admitted all exhibits presented. On their respective exhibit lists, the Parties reference the dockets for the search warrants. (See ECF Nos. 96, 97.) The July 20, 2018 Cell Phones Warrant Application, the accompanying Gonzalez Affidavit, and the Cell Phones Warrant can be found at Docket No. 3:18sw180, ECF Nos. 1, 1-1, and 4.

<sup>9</sup> During the time covered by the Superseding Indictment, V1 turned fourteen.

The Gonzalez Affidavit describes the end of Skinner and V1's relationship. After V1 attempted to end their sexual relationship, Skinner "started harassing her and attempting to manipulate her with threats of suicide." (Gonzalez Aff. ¶ 39.) V1 eventually cut off contact with Skinner, but she was contacted by another online persona, "Tiramisu," who V1 suspected was an alter-ego of Skinner. (*Id.*)

The Gonzalez Affidavit states that based on his review of documents recovered from Skinner at the time of his arrest and store surveillance footage, Skinner departed Auckland, New Zealand on June 20, 2018, and arrived in Richmond, Virginia on June 21, 2018. (*Id.* ¶ 41.) On June 22, 2018, after spending the night at a hostel in Richmond, Skinner traveled to the Walmart Supercenter in Glen Allen, Virginia, where he made two separate purchases for: (1) pepper spray; and, (2) a clip (folding) knife and duct tape. (*Id.*)

Later that afternoon, Skinner traveled to V1's family home in Goochland, Virginia. (*Id.* ¶ 42.) V1 [REDACTED]

[REDACTED] Upon arriving at her residence, Skinner "attempted to gain entrance to the residence through a basement door." (*Id.*) Alarmed, V1, her mother, and her sister retreated upstairs where V1's mother, after calling V1's father on his phone, retrieved a handgun. (*Id.*) Despite verbal warnings from V1's mother to leave, Skinner proceeded to a different entrance, broke a glass panel, and placed his "upper body . . . inside the door in an attempt to unlock it." (*Id.*) V1's mother shot the handgun, striking Skinner in the neck. (*Id.*)

Shortly thereafter, members of the Goochland County Sheriff's Office arrived at V1's home and found Skinner lying in a neighbor's yard. (*Id.* ¶ 43.) When a deputy sheriff asked Skinner what had happened, Skinner replied that "he was shot while trying to break the window to the door, and further that he was trying to break the window to get to his girlfriend." (*Id.*)

Underneath Skinner's sweatshirt, which lay several feet away from him, law enforcement found "a knife, which was open and in an extended position." (*Id.*) "Officers also found a backpack . . . which they connected to [Skinner]." (*Id.*) A search of the backpack revealed a "roll of duct tape." (*Id.*) "Investigators also recovered from Skinner a small canister of pepper spray, as well as a hand-written checklist of items to bring, which included pepper spray and duct tape." (*Id.*) They found a receipt for the purchase of many of those items from a nearby Walmart in Glen Allen, Virginia. (*Id.* ¶¶ 40–41.) Law enforcement also recovered from Skinner the two subject cell phones, "which investigators seized for evidentiary purposes and later turned over to the FBI." (*Id.*)

The Gonzalez affidavit describes details of the parties' communications obtained after the attempted break in. [REDACTED]

[REDACTED]

[REDACTED]





---

<sup>10</sup> Today's Constitutional Motions Decision reveals in detail contents of several conversations, photographs, and videos. Some of these items were obtained from the search of Skinner's cell phones, and some from his Gmail accounts. While those facts pertain to, and are incorporated into, the Motion to Suppress—especially those found on the cell phones because they served as a basis to search Skinner's Gmail accounts—the Court will not repeat those contents in detail here.

[REDACTED]

Following the chat session in which the second photograph was taken, Skinner “sent V1 that photograph through the Discord application.” (*Id.*)

In sum, in relation to the child pornography charges, the Gonzalez Affidavit presented sworn information seeking to demonstrate that Skinner had engaged in a sexual relationship with a minor on an online platform and that he had photographed, videotaped, and otherwise memorialized those sexual encounters. The Gonzalez Affidavit determined that evidence of these online sexual encounters with a minor would be found on Skinner’s cell phones based on:

(1) V1’s minor status; (2) an independent review of V1’s cell phone and Discord chats with Skinner; (3) an interview with V1 [REDACTED]

[REDACTED] (5) Skinner’s statements that he was trying to reach his minor girlfriend at the time of his capture; (6) [REDACTED]

[REDACTED] the circumstances and nature of which officers believed constituted child pornography.

### 3. The Search Process

The Gonzalez Affidavit included introductory information regarding his background, a report of the statutory provisions, an explanation of technical terms, a description of typical characteristics of collectors of child pornography, and a narrative of how and why the forensic search and analysis requires an image and complex search upon seizure. (Gonzalez Aff.

¶¶ 7-12.) Regarding search protocol, Gonzalez stated that computer files on a cell phone’s internal memory or SIM card, or their remnants, can be recovered months after they have been

downloaded. (*Id.* ¶ 25.) The Affidavit identified Discord as an application designed for gaming communities to text, video, or talk over a chat channel. (*Id.* ¶ 15(i).)

The Gonzalez Affidavit explained that the forensic analysis sought, including non-user generated evidence, can show how a computer has been used, what it has been used for, and who has used it. (*Id.* ¶ 28.) Gonzalez analogizes this “user attribution” evidence to a “search for ‘indicia of occupancy’ while executing a search warrant at a residence.” (*Id.* ¶ 28(b).) The Gonzalez Affidavit makes clear that a forensic analysis can show who has controlled the device and demonstrate the timing of file creation or chats by examining deleted files or “cache” files (those viewed on the internet sometimes automatically downloaded in a temporary directory). (*Id.*)

With that background, the Gonzalez Affidavit indicated that, depending on the volume of stored data, the dynamic review of the information necessary to draw an accurate conclusion, and the forensic tools necessary to evaluate a device’s particular configurations, could take weeks or months, and “would be impractical and invasive to attempt on-site.” (*Id.* ¶ 29(a).) The Gonzalez Affidavit also explained that while “it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators,” because reviewing the data in context, including whether counter-forensic programs exist, requires specialized knowledge about “how a computer behaves.” (*Id.* ¶ 28(d).)

**4. Items Sought to be Seized**

Attachment B to the Cell Phones Warrant identified items subject to search, including but not limited to records falling within ten identified categories:

- a) Any and all visual depictions of minors;
- b) Any and all communications with minors;
- c) Any and all communications with other individuals about Victim 1;
- d) Any and all communications with other individuals that discuss TROY GEORGE SKINNER's plan to travel, or which discuss his actual travel, from New Zealand to the Richmond, Virginia area, which travel occurred during June 2018;
- e) Any and all address books, names, and lists of names and addresses of minors;
- f) Any and all diaries, notebooks, notes, and any other records reflecting physical contact, whether real or imagined, with minors, and any such items discussing sexual activities with minors;
- g) Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;
- h) All records and information relating to any and all Discord accounts/usernames used by TROY GEORGE SKINNER, including but not limited to godot#6615 and any account incorporating Tiramisu in its name;
- i) All records and information relating to the location, past or present, of TROY GEORGE SKINNER; [and,]
- j) All records relating to TROY GEORGE SKINNER's Internet search and online shopping histories.

(Gonzalez Aff. Attach. B.) On July 20, 2018, then-Magistrate Judge David J. Novak approved the warrant application, and commanded law enforcement to execute the warrant on or before July 30, 2018.<sup>11</sup> The Cell Phones Warrant did not include a date restriction for the files to be searched.

---

<sup>11</sup> Skinner remain hospitalized from June 22, 2018 until July 22, 2018 for his gunshot wounds. (Feb. 13, 2020 Hr'g Tr. 15.)

Five days later, on July 24, 2018, law enforcement executed the Cell Phones Warrant. Following a search of Skinner's Huawei cell phone for the items identified in Attachment B to the Cell Phones Warrant, the government identified a movie file entitled "Desktop 02.06.2018-03.16.130100.DVR.mp4," which was created on or about February 5–6, 2018. Forensic analysis revealed that the movie was downloaded to the phone from one of Skinner's email accounts (johnvlogchamber@gmail.com). The movie, which lasts six minutes, [REDACTED]

[REDACTED] V1 was unaware that Skinner created any video content during their online communication. (Aug. 6, 2020 Hr'g Tr. 49; U.S. Ex. 15.) This video file serves as the basis for Count Seven in the Superseding Indictment.

#### **5. The October 12, 2018 Johnvlogchamber Gmail Warrant**<sup>12</sup>

On October 12, 2018, FBI Special Agent Kathryn Weber submitted applications for two warrants to search two separate email accounts associated with Skinner. (*See* 3:18sw267; 3:18sw268.) Special Agent Weber based these applications on a 17–page affidavit (the "Weber Affidavit"), similar to the affidavit submitted by Special Agent Gonzalez, which described the potential violations of the same four criminal statutes delineated in the Cell Phones Warrant. The first of these warrants sought to search the johnvlogchamber Gmail account. (Weber Aff., No. 3:18sw267, ECF No. 1.)

Because the Huawei cell phone had information related to a johnvlogchamber@gmail.com account, Agent Weber sought a search warrant for that email account. In substantially similar terms as the Gonzalez Affidavit, the Weber Affidavit detailed

---

<sup>12</sup> During the February 13, 2020 Evidentiary Hearing, the Court admitted all exhibits presented. (*See* ECF Nos. 96, 97.) The October 12, 2018 Johnvlogchamber Gmail Warrant Application, the Weber Affidavit, and the Johnvlogchamber Gmail Warrant can be found at Docket No. 3:18sw267, ECF Nos. 1 and 4.

Skinner and V1's online relationship, the CAFI interview evidence, and Skinner's travel to the United States where he attempted breaking into V1's house while carrying a knife, and which led to his arrest on June 22, 2018. (*See* Weber Aff. ¶¶ 28–38.) The Weber Affidavit also described the evidence of production of child pornography seized from Skinner's cell phone. Specifically, Special Agent Weber swore that her review of Skinner's Huawei mobile phone [REDACTED]

[REDACTED] Weber stated the file path for the video was listed as Google Drive Files and affiliated with johnvlogchamber@gmail.com. (*Id.* ¶ 40.) Based on her discussions with "FBI digital forensic analysts," Agent Weber stated that "this file path information indicates that this child pornography video was downloaded to the phone on June 19, 2018, from the Google Drive for account user johnvlogchamber@gmail.com." (*Id.*) Attachment B described the particular items to be seized and permitted the seizure of items relating to the listed criminal violations occurring after December 25, 2017 until the date of the warrant. (Weber Aff., Johnvlogchamber Gmail Warrant Attach. B 1–3.) The Weber Attachment B identified the eleven items subject to search, including some specific to V1:

- a) All contact information, including full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- b) All records pertaining to other accounts with which SUBJECT ACCOUNTS may have shared Google Drive content, specifically video and/or picture content;
- c) Any and all visual depictions of minors;
- d) Any and all communications with minors, both public and private messages;

- e) Any and all communications with other individuals about Victim 1, both public and private messages;
- f) Any and all documents and communications relating to the manner and means of abduction and kidnapping another person, including: 1) tools and techniques for gaining access to buildings, vehicles and separately secured containers; 2) tools and techniques for restraining individuals; and, 3) information about torture and methods of disposing of bodies;
- g) Any and all documents relating to TROY GEORGE SKINNER's plans to travel, or his actual travel, from New Zealand to the Richmond, Virginia area, including any communications with other individuals about his travel, information and or documents relating to methods and means of travel, lodging, points of interest, and safety and security while traveling, including but not limited to personal safety and information security;
- h) All records or other information stored by an individual using the account, including address books, contact and buddy lists, servers the user participates in, pictures, and files;
- i) Any and all communications, notes, and any other records reflecting physical contact, whether real or imagined, with minors, and any such items discussing sexual activities with minors;
- j) Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids; and,
- k) All records and information relating to the location, past or present, of TROY GEORGE SKINNER.

(*Id.*)

On October 12, 2018, then–Magistrate Judge Roderick C. Young approved the Johnvlogchamber Gmail Warrant, and commanded law enforcement to execute the warrant on or before October 26, 2018. (3:18sw267, ECF No. 4.)

**6. The October 12, 2018 Lottic.ysw Gmail Warrant**<sup>13</sup>

Also on October 12, 2018, Special Agent Weber submitted a second warrant application, relying on the 17–page Weber Affidavit, seeking to search a separate email account associated with Skinner: lottic.ysw@gmail.com. Similar to the affidavit submitted by Special Agent Gonzalez for the Cell Phones Warrant, Weber described the potential violations of the same four criminal statutes. In support of the Lottic.ysw Gmail Warrant, the Weber Affidavit stated that a search of Skinner’s Samsung mobile phone “resulted in the identification of several emails either to or from SUBJECT ACCOUNT lottic.ysw@gmail.com that constitute evidence pertinent to the offenses listed above . . . including [an email referencing an address in Goochland,] which I know from my investigation to be the home address of V1.” (Weber Aff. ¶ 41; Case No. 3:18sw268, ECF No. 1.)

On October 12, 2018, then-Magistrate Judge Young approved the Lottic.ysw Gmail Warrant, and commanded law enforcement to execute the warrant on or before October 26, 2018. The Lottic.ysw Gmail Warrant contained a three-page Attachment B—identical to the Attachment B in the Johnvlogchamber Gmail Warrant—identifying the items subject to search. Attachment B described the items to be seized and permitted the seizure of items relating to the listed criminal violations occurring after December 25, 2017 until the date of the warrant. (3:18sw268, ECF No. 4.)

**7. Executing the Warrants**

On October 12, 2018, Special Agent Weber uploaded the Johnvlogchamber Gmail and the Lottic.ysw Gmail Warrants to “Google’s law enforcement request system” or “LERS.” (Feb.

---

<sup>13</sup> As noted earlier, the Court admitted all exhibits presented during the First Evidentiary Hearing. (See ECF Nos. 96, 97.) The October 12, 2018 Lottic.ysw Gmail Warrant Application, the Weber Affidavit, and the Lottic.ysw Warrant can be found at Docket No. 3:18sw268, ECF Nos. 1 and 4.



13, 2020 Hr’g Tr. 44, ECF No. 100.) According to a screenshot of Google’s LERS entry, Special Agent Weber uploaded both Gmail Warrants with Attachment A (the “Property to be Searched”) describing each Gmail Account and Attachment B (the “Particular Things to be Seized”). (Feb. 13, 2020 Hr’g, U.S. Ex. 10.) There is no indication that the Weber Affidavit also was sent via the LERS. (Feb. 13, 2020 Hr’g, U.S. Ex. 10.)

Following a search of the Johnvlogchamber Gmail account for the items identified in Attachment B to the Gmail Warrants, the Government identified an image file entitled “20180223\_120558.jpg,” which was created on or about February 22–23, 2018. The image file is a photograph of [REDACTED] This image file serves as the basis for Count Eight in the Superseding Indictment.

Following a search of the Lottic.yzw Gmail account for the items identified in Attachment B to the Gmail Warrants, the Government identified a movie file entitled “2018-03-05 17-50-35.flv,” which was created on or about March 4–5, 2018. The movie, which lasts 6 minutes and 43 seconds, depicts [REDACTED]  
[REDACTED]  
[REDACTED] This movie has a screen-in-screen display showing Skinner’s face. This video file serves as the basis for Count Nine in the Superseding Indictment.

## **II. Analysis**

Skinner contends that the Cell Phones and Gmail Warrants “were essentially general warrants” that failed to establish probable cause sufficient to authorize a wholesale search for all information on the phone or in the accounts.” (Mot. Suppress 2.) Skinner raises important questions with which courts have increasingly struggled as the power of electronic information

gathering and storage has grown exponentially. Courts are increasingly called to balance constitutional protection of privacy from improper governmental intrusion against a nearly unimaginable amount of information electronic devices store. This Gordian Knot grows tighter because courts are called to weigh this intrusion by the government when it seeks information whose availability—as well as the mechanism of collection and storage—remains in the possession of private sector companies that law enforcement agencies do not regulate or control.

Constitutional and common law rarely answer these questions precisely, and the swift development of technology can suggest different answers as technology advances. “As always, ‘the ultimate touchstone of the Fourth Amendment is reasonableness.’” *United States v. Cobb*, 970 F.3d 319, 327 (4th Cir. 2020), as amended (Aug. 17, 2020) (citations omitted). As explained below, the Court must deny Skinner’s Motion to Suppress.

**A. Probable Cause Existed for the Three Warrants**

Because the singular facts here and controlling law require it, the Court determines that probable cause supported the warrants, which were sufficiently particular, narrowly tailored, and timely. Even if they were not, the good-faith exception would apply to the officers’ actions. As such, the Court will deny Skinner’s Motion to Suppress on these grounds.

**1. Legal Standard: The Warrant Requirement**

The Fourth Amendment mandates that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. AMEND. IV. The Warrant Clause encompasses two

“related but distinct concepts: particularity and breadth.” *United States v. Manafort*, 323 F. Supp. 3d 795, 801 (E.D. Va. 2018) (internal citation omitted).

**a. Particularity**

The Framers included the particularity requirement to “to end the practice, abhorred by the colonists, of issuing general warrants,” which authorized officers to carry out an “exploratory rummaging in a person’s belongings.” *United States v. Dargan*, 738 F.3d 643, 647 (4th Cir. 2013) (internal citation and quotations omitted). “The Fourth Amendment ‘specifies only two matters that must be ‘particularly described’ in the warrant: ‘the place to be searched’ and ‘the persons or things to be seized.’” *Cobb*, 970 F.3d at 327 (quotations and citations omitted). “So long as the warrant describes the items to be seized with enough specificity that the executing officer is able to distinguish between those items which are to be seized and those that are not . . . the particularity standard is met.” *United States v. Blakeney*, 949 F.3d 851, 862 (4th Cir. 2020) (internal citations and quotations omitted). A warrant is sufficiently particular when it “confine[s] the executing [officers’] discretion by allowing them to seize only evidence of a particular crime.” *Cobb*, 970 F.3d at 328 (quoting *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986)).

Despite the need to confine the discretion of the executing officers, warrants “should be read with a commonsense and realistic approach,” *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (internal citations omitted), and courts should avoid hyper-technical interpretations of warrants which might “impose a ‘constitutional strait jacket’” on investigating officers, *Dargan*, 738 F.3d at 647. The particularity requirement thus forbids fishing expeditions “while simultaneously preserving the flexibility of law enforcement to adapt to the unforeseen circumstances that necessarily arise in an investigation predicated on incomplete

information.” *Id.* The United States Court of Appeals for the Fourth Circuit has long recognized that “in most cases, ‘a [w]arrant need not—and in most cases, cannot—scrupulously list and delineate each and every item to be seized’” because it is frequently “impossible for law enforcement officers to know in advance exactly what . . . records the defendant maintains or how the case against him [or her] will unfold.” *Cobb*, 970 F.3d at 327–28. Indeed, where a warrant does not *otherwise* describe the evidence to be seized, sometimes that gap can be filled if the warrant instead specifies the relevant offense.” *Id.* at 328 (quoting *Blakeney*, 949 F.3d at 862–63) (additional citations omitted). The particularity requirement “is fulfilled when the warrant identifies the items to be seized by their relation to designated crimes and when the description of the items leaves nothing to the discretion of the officer executing the warrant.” *Williams*, 592 F.3d at 519 (citation omitted).

“As a general rule, a supporting affidavit or document may be read together with (and considered part of) a warrant that otherwise lacks sufficient particularity ‘if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant.’” *United States v. Hurwitz*, 459 F.3d 463, 470–71 (4th Cir. 2006) (quoting *Groh v. Ramirez*, 540 U.S. 551, 557 (2004)). Particularity may be satisfied where the warrant “cross-references” or “incorporates” the affidavits and other supporting documents. *Hurwitz*, 459 F.3d at 473 (quoting *Groh*, 540 U.S. at 557 (2004)). The Fourth Circuit deems it “sufficient either for the warrant to incorporate the supporting document by reference or for the supporting document to be attached to the warrant itself.” *Id.*

**b. Breadth**

The breadth requirement ensures that the “scope of the warrant [is] limited by the probable cause on which the warrant is based.” *Manafort*, 323 F. Supp. 3d at 801 (internal

quotation marks and citation omitted). Probable cause to search exists if there is “a fair *probability* that contraband or evidence of a crime will be found in a particular place.” *United States v. Bynum*, 604 F.3d 161, 165 (4th Cir. 2010) (emphasis in original) (internal quotation marks and citation omitted).

The judicial officer’s determination of probable cause is a “practical, common-sense decision . . . given all the circumstances set forth in the affidavit,” *United States v. Montith*, 662 F.3d 660, 664 (4th Cir. 2011) (internal quotation marks and citation omitted), and that determination is “entitled to ‘great deference’ by a reviewing court,” *United States v. Abramski*, 706 F.3d 307, 318 (4th Cir. 2013). The court must therefore limit its inquiry to assessing “whether the magistrate judge had a ‘substantial basis’ for concluding that probable cause existed.” *Id.* at 314 (quoting *Illinois v. Gates*, 462 U.S. 213, 238–39 (1983)). Whether the issuing judge had a substantial basis for finding probable cause is reviewed under the totality of the circumstances. *United States v. May*, 446 Fed. App’x 652, 654 (4th Cir. 2011). “As always, the ultimate touchstone of the Fourth Amendment is reasonableness.” *Cobb*, 970 F.3d at 327.

Courts, including the Fourth Circuit, encourage a balance between refusing fishing expeditions and permitting flexibility in the reading of search warrants. A commonsense approach to interpretation of warrants encourages officers to seek judicial approval before conducting a search that would intrude on constitutionally protected domains. *Dargon*, 738 F.3d at 647 (citation omitted).

In sum, particularity requires that the items to be seized are clearly listed in the warrant, while the breadth requirement commands that probable cause exist for the items that are listed.

And to the extent ambiguity exists, clarification can be drawn from the offenses identified in the warrant.

**2. The Warrants Did Not Lack Particularity or Probable Cause**

The Court will deny Skinner's Motion to Suppress. As a threshold matter, the Court determines that under Fourth Circuit law, the warrants must be read alongside the supporting affidavits because the warrants used sufficient terms of incorporation. Having resolved this, the Court concludes that the warrants adequately identified the items to be searched, and that the reviewing Magistrate Judges possessed substantial grounds for their determination of probable cause. Finally, even if the warrants fell short of either of these prerequisites, the officers acted in good-faith reliance on the Magistrate Judges' approval of the warrants.

**a. All Three Warrants Should Be Read Together With Their Supporting Affidavits Because the Affidavits Were Referenced in the Warrants and the Warrants Used Sufficient Terms of Incorporation**

Skinner contends that the warrants cannot be read together with the supporting affidavits, stating that the government cannot "shore up the defects in the warrants' lack of particularity by asking the Court to rely on the information contained in the affidavits in support of the search warrants." (Skinner Reply Mot. Suppress 1, ECF No. 92.) Skinner's arguments cannot prevail. In the Fourth Circuit, it "is sufficient either for the warrant to incorporate the supporting document by reference or for the supporting document to be attached to the warrant itself."<sup>14</sup> *Hurwitz*, 459 F.3d at 473. Here, as required in the Fourth Circuit, both the Cell Phones Warrant and the Gmail Warrants incorporated by reference the affidavits in support of them.

---

<sup>14</sup> The Fourth Circuit has recognized "that a majority of our sister Circuit Courts of Appeals appear to require the satisfaction of both conditions before allowing a separate document to be read as part of the search warrant." *Hurwitz*, 459 F.3d at 471.

The first page of the Cell Phones Warrant states that the Magistrate Judge “find[s] that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above.” (*See* Cell Phones Warrant 1, 3:18sw180, ECF No. 4.) The Cell Phones Warrant continues that the “search will identify” the items outlined in “Attachment B.” (*Id.*) The Cell Phones Warrant thus directly incorporates both the Gonzalez Affidavit and Attachment B, which limits the evidence to be searched to “[a]ll records and information” relating to the violation of four criminal statutes. (Cell Phones Warrant, Attach. B 1.)

The same holds true for the Gmail Warrants. Both Gmail Warrants state that the Magistrate Judge “find[s] that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.” (*See* Johnvlogchamber Gmail Warrant 1, 3:18sw267, ECF No. 4; Lottic.ysw Gmail Warrant 1, 3:18sw268, ECF No. 4.) Each of the Gmail Warrants directs that Attachment A (specifying the “Property to be Searched”) and Attachment B (specifying the “Particular Things to be Seized”) are “fully incorporated by reference herein.” (*Id.*) The Gmail Warrants thus directly incorporate the Weber Affidavit and Attachments A and B.<sup>15</sup>

In sum, all three search warrants explicitly incorporate the respective affidavits by reference, and attached the supporting documents describing the items to be seized in relation to the specific criminal statutes law enforcement believed Skinner had violated. Each search

---

<sup>15</sup> The Court heard testimony at the February 13, 2020 Evidentiary Hearing that Attachments A and B of the Gmail Warrants were attached to the search warrants at the time of their execution. During the hearing, Special Agent Weber testified that, after Magistrate Judge Young approved the Gmail Warrants, she uploaded them through Google’s Law Enforcement Request or LERS system. (Feb. 13, 2020 Hr’g Tr. 43.) The United States also introduced into evidence a screenshot of Special Agent Weber’s upload to the LERS system of the Gmail Warrants. The screenshot shows that Special Agent Weber uploaded both Gmail Warrants along with Attachment A (the “Property to be Searched”) describing each Gmail Account and Attachment B (the “Particular Things to be Seized”). (*See* U.S. Ex. 10, ECF No. 96.) The copy of the Gmail Warrants uploaded to the LERS system did not include the Weber Affidavit.



warrant incorporated by reference either Agent Gonzalez or Agent Weber's affidavit, thus avoiding any difficulty with the Supreme Court's decision in *Groh v. Ramirez*, 540 U.S. 551 (2004). *See Hurwitz*, 459 F.3d at 470–71 (“As a general rule, a supporting affidavit or document may be read together with (and considered part of) a warrant that otherwise lacks sufficient particularity ‘if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant.’” (quoting *Groh*, 540 U.S. at 557–58)). These documents may be fairly considered along with the warrants in establishing particularity and probable cause.

**b. The Cell Phones Warrant Was Sufficiently Particular and Not Overly Broad Because It Adequately Identified the Items to Be Searched and Provided Overwhelming Probable Cause**

Skinner seeks to suppress evidence obtained from the Cell Phones Warrant. His argument is twofold. First, he contends that the Cell Phones Warrant fails to meet the particularity requirement of the Fourth Amendment, and thus amounts to a general warrant. Second, Skinner argues that the scope of the Cell Phone Warrant exceeded the probable cause available to officers and the Magistrate Judge at the time the Magistrate Judge issued the Cell Phones Warrant. Because the Gonzalez Affidavit and the Cell Phones Warrant as a whole established a substantial basis to believe evidence of specific criminal conduct would be found on Skinner's cell phones and limited the search to evidence of that criminal conduct, the Court must reject both these contentions in turn.

**i. The Cell Phones Warrant Was Sufficiently Particular**

The Cell Phones Warrant adequately “confine[d] the executing [officers'] discretion by allowing them to seize only evidence of [] particular crime[s].” *United States v. Cobb*, 970 F.3d at 328 (quoting *Fawole*, 785 F.2d at 1144). Specifically, Attachment B of the Gonzalez Affidavit, which was incorporated into the Cell Phones Warrant, limited the items to be seized to



“[a]ll records and information relating to . . . attempted kidnapping . . . production of child pornography . . . distribution, receipt, and possession of child pornography . . . and online enticement.” (Gonzalez Aff., Attach. B 1.) While a warrant authorizing a search for evidence relating to broad criminal statutes such as “wire fraud” or “tax evasion” may be insufficiently particular, that is not the case with regard to these child pornography and kidnapping charges. *United States v. Dickerson*, 166 F.3d 667, 694 (4th Cir. 1999) (judgment reversed on Fifth Amendment grounds) (quoting *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992)). A warrant is sufficiently particular when it “confine[s] the executing [officers’] discretion by allowing them to seize only evidence of a particular crime.” *Cobb*, 970 F.3d at 328 (quoting *Fawole*, 785 F.2d at 1144)).

Certainly the search for child pornography distribution and production, and kidnapping, sufficiently “limited the agents’ search to evidence relating to the commission” of four particular crimes that would, by their nature, “generate[] quite distinctive evidence.” *Dickerson*, 166 F.3d at 694. These statutory limitations adequately distinguished between the materials to be searched and seized and those which were to be left undisturbed by law enforcement. As the Fourth Circuit has stated, “[m]ore specificity is not required by the Constitution.” *United States v. Ladd*, 704 F.2d 134, 136 (4th Cir. 1983).

In addition, the Cell Phones Warrant described the items to be seized with enough specificity that an executing officer could distinguish those items from those that do not constitute materials related to the alleged offenses. This meets the particularity standard. *Blakeney*, 949 F.3d at 862 (internal quotation marks and citations omitted). A warrant may satisfy the particularity requirement where it contains a description of items to be seized “delineated in part by an illustrative list of seizable items.” *Manafort*, 323 F. Supp. 3d at 802

(quoting *United States v. Riley*, 906 F.2d 841, 844–45 (2d. Cir. 1990)). The Gonzalez Affidavit identified ten categories of material to be searched on the cell phones. For the potential child pornography offenses, the Cell Phones Warrant authorized searching for “[a]ny and all visual depictions of minors” and “any and all communications with other individuals about Victim 1.” (Cell Phones Warrant Attach. B.) For the kidnapping offenses, the Cell Phone Warrant authorized searching for “communications . . . [relating to Skinner’s] plans to travel, or which discuss his actual travel, from New Zealand to the Richmond, Virginia area.” (*Id.*) Given these specific categories of items to be searched and seized, it cannot be said that the Cell Phones Warrant authorized a general rummaging in Skinner’s belongings.

Skinner contends that the provisions authorizing the search of “all records and information relating to the location, past or present, of TROY GEORGE SKINNER” and “[a]ll records relating to Troy George Skinner’s Internet search and online shopping histories” were insufficiently particular. (*Id.*). While these categories are admittedly broad, their presence does not invalidate the Cell Phone Warrant for three reasons.

First, those categories must be read in tandem with the section limiting the items to be searched to those relating to the four possible criminal violations. Relevant here, “a warrant that describes the items subject to seizure in broad, generic terms can be valid if the description is as specific as the circumstances and the nature of the activity under investigation permit.”<sup>16</sup>

---

<sup>16</sup> Similarly, the United States Court of Appeals for the Second Circuit discussed in *Ulbricht* how search warrants involving digital media do not require a perfect description of the data to be constitutionally searched and seized:

Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. A general search of electronic data is an especially potent threat to privacy because hard drives and e-mail accounts may be akin to a residence in terms of the scope and quantity of private information they may contain. The seizure of a computer hard drive, and its subsequent retention by the government, can therefore give the government

*Manafort*, 323 F. Supp. 3d at 803 (internal quotation marks and citations omitted). For the Cell Phones Warrant, the circumstances and the nature of the activity required reviewing information related to child pornography and kidnapping which may have come from different media or files on the two cell phones. Moreover, the Cell Phones Warrant did not authorize law enforcement to search for *any* location information or *any* records relating to Skinner’s online shopping or location, but merely those records relating to the four criminal categories. Courts have upheld similar searches of online data for location information when relevant to the criminal conduct alleged. *See Ulbricht*, 858 F.3d at 104 (finding search for “any evidence concerning [defendant’s] travel or patterns of movement” sufficiently particular when limited by enumerated criminal statutes”). Accordingly, the Cell Phones Warrant’s authorization of seizure of [a]ll records and information relating to . . . attempted kidnapping . . . production of child pornography . . . distribution, receipt, and possession of child pornography . . . and online enticement,” (Gonzalez Aff., Attach. B 1), was sufficiently specific given the nature of the offenses at issue here.

---

possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure. Such sensitive records might include tax records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, and banking and shopping information. Because of the nature of digital storage, it is not always feasible to extract and segregate responsive data from non-responsive data, creating a serious risk that every warrant for electronic information will become, in effect, a general warrant. Thus, we have held that warrants that fail to link the evidence sought to the criminal activity supported by probable cause do not satisfy the particularity requirement because they lack meaningful parameters on an otherwise limitless search of a defendant’s electronic media.

*United States v. Ulbricht*, 858 F.3d 71, 99–100 (2d Cir. 2017) (internal quotation marks, alterations, and citations omitted), abrogated by *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

Second, Skinner's shopping history and location were plainly relevant to the criminal statutes named in the Cell Phones Warrant. The FBI determined that Skinner had purchased several items to prepare for the alleged kidnapping and had traveled from New Zealand to the United States. (*See* Gonzalez Aff. ¶¶ 40–41 (describing Skinner's travel from New Zealand to Richmond and his purchases of duct tape, a clip knife, and pepper spray at the Walmart in Glen Allen).) Internet search and shopping history would be relevant to any attempts on Skinner's part to purchase or otherwise find child pornography. Because the Cell Phones Warrant had already limited the search to those items related to particular crimes—production of child pornography, possession of child pornography, enticement, and kidnapping—it would be impracticable to further narrow the items to be examined in Skinner's search history and online purchases.

Third, law enforcement must be afforded a certain amount of leeway when conducting internet and computer searches pursuant to a warrant. In the context of computer searches, as with paper documents, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *Andresen v. Maryland*, 427 U.S. 463, 482 (1976). In decisions to be addressed more fully below, the Fourth Circuit has, more than once, recognized the need for law enforcement to conduct a cursory review of some files on Skinner's cell phones even if they were not labeled "child pornography" or "kidnapping plan." Limiting law enforcement's search, for instance, only to .jpg files that usually contain images would risk overlooking key pieces of evidence, as "the designation or labeling of files on a computer can easily be manipulated to hide their substance." *Williams*, 592 F.3d at 522; *see also United States v. Hill*, 459 F.3d 966, 974 (9th Cir. 2006) (noting that file designations such as "jpg" cannot be a limiting search term because those

suffixes can be manipulated); *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (“computer hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories”).


Here, law enforcement’s search of Skinner’s files for information relating to his location, shopping history, and online communications were relevant to both the kidnapping and child pornography charges and cabined by reference to the four criminal statutes stated in the warrant. Because the Cell Phones Warrant limited the ten itemized subjects to be searched on the two phones to those relating to four identified federal offenses and listed the items to be seized by reference to those offenses, the Court finds it meets the particularity requirement.


**ii. The Scope of the Cell Phones Warrant Was Supported by Substantial Probable Cause**

The Cell Phones Warrant satisfies the Fourth Amendment’s breadth requirement as it establishes probable cause that evidence of child pornography, coercion, and kidnapping would be found on Skinner’s cell phone. As stated above, the Cell Phones Warrant identifies four criminal statutes that law enforcement suspected Skinner of violating. The Cell Phones Warrant then listed ten categories of material to be searched for evidence of violations of those criminal statutes. These categories, rather than being overly broad, mirror the probable cause established by the Gonzalez Affidavit and the Cell Phones Warrant as a whole.

The Gonzalez Affidavit articulates sets forth a substantial basis, relying on at least seven different pieces of collected information, to believe that evidence of sexual images of a minor would be found on Skinner’s cell phone. The Cell Phones Warrant established probable cause that evidence of the production of child pornography would be found on Skinner’s cell phones because law enforcement had gathered the following information:


- (1) V1 was thirteen years old;
- (2) V1 had confirmed in an interview that Skinner used Discord on his cell phone and computer;

- 
- (5) An independent review of V1's cell phone and Discord chats with Skinner aligned with information in the interview;

- 
- (7) Skinner stated that he was trying to reach his minor girlfriend at the time of law enforcement found him.

(Gonzalez Aff. ¶¶ 31–43.)

The Cell Phones Warrant then closely tied the search of the cell phones to the probable cause laid out in the Gonzalez Affidavit. For instance, the Cell Phones Warrant authorized the search of “[a]ny and all communications with other individuals about [V1]” and “[a]ll records and information relating to any and all Discord accounts/usernames” utilized by Skinner. (Cell Phones Warrant, Attach. B 1.) These provisions track the facts established by the Affidavit



Furthermore, the Gonzalez Affidavit confirmed that “Skinner referenced using Discord on both his cellular telephone and his home computer.” (*Id.* ¶ 34.) These facts establish more than “a fair probability” or a substantial basis that a search of the cell phones for communications about V1 or information about Skinner’s Discord accounts would reveal information relating to the production of child pornography, especially when reviewing the warrant under the totality of the circumstances as the law requires. *May*, 464 F. App’x. at 654.

Similarly, the Cell Phones Warrant authorized searching for records and information relating to the following three categories involving the alleged potential kidnapping, including:

1. Any and all communications with other individuals that discuss TROY GEORGE SKINNER's plans to travel, or which discuss his actual travel, from New Zealand to the Richmond, Virginia area, which travel occurred during June 2018;
2. All records and information relating to the location, past or present, of Troy George Skinner; and,
3. All records relating to TROY GEORGE SKINNER's Internet Search and Online Shopping Histories.

(See Cell Phones Warrant Attach. B at 2–3.) Then–Magistrate Judge Novak reasonably concluded that probable cause existed to search Skinner's device for these provisions as well. As the Gonzalez Affidavit specifies, Skinner was found with duct tape, pepper spray, and a knife on his person after attempting to access V1's house. Skinner had traveled from New Zealand to Richmond, which required the purchase of numerous plane and bus tickets, as well as a hostel room in Richmond. (Gonzalez Aff. ¶ 40.) Skinner's communications concerning his travel, his location during the month of June, and his online shopping history were thus directly relevant to the kidnapping charges as reflected in the Cell Phones Warrant.

Finally, the Cell Phones Warrant authorized searching for records and information relating to the following five categories of evidence involving the production or possession of child pornography.

1. Any and all visual depictions of minors;
2. Any and all communications with minors;
3. Any and all address books, names, and lists of names and addresses of minors;



4. Any and all diaries, notebooks, notes, and any other records reflecting physical contact, whether real or imagined, with minors, and any such items discussing sexual activities with minors; and,
5. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

(See Cell Phones Warrant Attach. B at 2–3.) The Gonzalez Affidavit itemizes information establishing that Skinner possessed some quantity of child pornography on his electronic devices. [REDACTED]

[REDACTED] Thus, the Gonzalez Affidavit established that Skinner: (1) had corresponded extensively with a minor; (2) knew the minor was underage at the time; and, (3) had received numerous photographs that law enforcement determined, in their training and experience, depicted child pornography.

Skinner, however, contends that this information was insufficient to establish probable cause to search his phone for evidence of child pornography. Skinner challenges the section of the Gonzalez Affidavit entitled “Characteristics of Collectors of Child Pornography.” (Mot. Suppress 6.) In that section, Special Agent Gonzalez set out characteristics of child pornography collectors based off of his “knowledge, experience, and training in child pornography investigations.” (Gonzalez Aff. 6.) Skinner argues that this boilerplate “profile evidence” cannot be applied to him because nothing in the Gonzalez Affidavit places “Mr. Skinner within the collector profile described in the warrant.” (Mot. Suppress 5–6.)

This line of argument falters. First, the Magistrate Judge was justified in concluding that Skinner, due to his sexual relationship with a child during which they may have exchanged sexually explicit photographs, could fit the profile of a child pornography collector. For



instance, Special Agent Gonzalez that “[c]ollectors may receive sexual stimulation and satisfaction from contact with children.” (Gonzalez Aff. 6.) Skinner had received sexual stimulation from online encounters with a [REDACTED]. Based on the profile offered by the Gonzalez Affidavit probable cause existed that, Skinner, as someone who received sexual stimulation from his contact with V1, was likely to possess more child pornography and keep that child pornography on his person. As the search of one of Skinner’s cell phones revealed a [REDACTED], some aspects of the “collector” profile appear to fit Skinner’s actions and propensities. Given Skinner’s proven sexual stimulation from an encounter with a child, the Magistrate Judge was well within reason in concluding that Skinner fit the collector profile.<sup>17</sup>

Second, even if Skinner did not fit the profile of a “collector” as set out in the Gonzalez Affidavit, the Cell Phones Warrant would still provide ample probable cause to search Skinner’s cell phones for evidence of additional child pornography involving V1. The Gonzalez Affidavit set out more than a “fair probability”—and more than a substantial basis—that there would at least be some child pornography on Skinner’s phone. *Bynum*, 604 F.3d at 165. Law enforcement had seen child pornography from Skinner’s online Discord account and confirmed that Skinner had accessed that child pornography [REDACTED]. Skinner, then, at best can argue that it was unlikely that there were pictures of and communications with

---

<sup>17</sup> Skinner argues that he could not possibly fit the collector profile because [REDACTED]

[REDACTED]

But as discussed in the Constitutional Motions Decision issued in conjunction with this decision, no party disputes that Skinner had knowledge of V1 being under the age of eighteen throughout the course of their interactions. And Skinner does not contest that V1 presented as a [REDACTED] in the United States.

other minors who were not V1 on the phone. But warrants “should be read with a commonsense and realistic approach.” *Williams*, 592 F.3d at 519 (internal quotation marks and citation omitted). Here, many of the images [REDACTED]

Practically, then, a search solely for images of V1 would leave law enforcement unable to determine whether some (faceless) pornographic images of children depicted V1 or another minor.<sup>18</sup>

As the Supreme Court has noted, “[p]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” *Gates*, 462 U.S. at 232. At its most general, probable cause “exists if it would be reasonable to seek the evidence in the place indicated in the affidavit.” *United States v. Adjani*, 452 F.3d 1140, 1145 (9th Cir. 2006) (internal quotation marks and citations omitted). Here, the Magistrate Judge reasonably concluded that the evidence showing Skinner possessed sexual images of a child raised a fair probability that other evidence of child pornography would be found on Skinner’s cell phone. The Court, paying the appropriate “great

---

<sup>18</sup> Moreover, courts have upheld searches for evidence of child pornography where the affidavit only establishes the existence of a few items of child pornography, or child pornography involving one person. See *United States v. Shelton*, 418 F. App’x 514, 518 (7th Cir. 2011) (finding that a description of a file on a computer depicting “a 12-year-old girl undressing to a state of complete nudity in a bedroom—provides common sense support that the computer might contain child pornography”); *United States v. Keith*, 183 F. Supp. 3d 427, 432 (S.D.N.Y. 2016) (explaining that a “single instance of possession or receipt of child pornography” may be sufficient probable cause to search for more “if circumstances suggest that the suspect had accessed those images willfully and deliberately”); *United States v. Jarman*, 61 F. Supp. 3d 598, 606 (M.D. La. 2014) (finding probable cause to search computer for evidence of child pornography where a private computer technician had discovered “an ‘image of an adult sodomizing a prepubescent male’”); *United States v. Davies*, No. 3:08cr00253, 2010 WL 3024844, at \*4 (M.D. Pa. July 29, 2010) (finding “sufficient evidence to give rise to probable cause to believe that Defendant attempted to produce and/or possess child pornography” where “Defendant engaged in explicit online discussions with [an agent pretending to be a minor] said he wanted to take pictures of her on his pool table, asked her to take off her hoodie and shirt in subsequent photographs, and then gave her his address”).

deference” to the Magistrate Judge’s conclusion, cannot disturb that judgment. *Gates*, 462 U.S. at 232.

**iii. The Cell Phones Warrant Was Not Overbroad**

Skinner adds a more fundamental challenge to the Cell Phones Warrant. He argues that, given the nature of computer searches and the ubiquity of private information on a person’s phone, the overbreadth of the search violated his right to privacy. (Mot. Supp. 4.) Echoing the 2015 *Riley* decision from the United States Supreme Court, Skinner notes that “‘there is an element of pervasiveness that characterizes cell phones but not physical records . . . [a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.’” (*Id.*) (quoting *Riley v. California*, 134 S. Ct. 2473, 2490, 2491 (2015)). He emphasizes that particularity and overbreadth are related concepts. (*Id.*)

The crux of much of Skinner’s argument is that searching computers without proper limitations—given how much information electronic devices can contain—amounts to a general warrant. Skinner also seems to suggest that law enforcement, rather than the itemization utilized, should have also described the “types of files sought, the location of the files, the timeframe [and] the relationship between the files and the information” that Gonzalez had about the crime.<sup>19</sup> *Cobb*, 970 F.3d at 328. Skinner asks for limitations concerning the specific files searched rather than “generic classifications.” (Mot. Suppress 5–6.)

---

<sup>19</sup> Judge Floyd’s thoughtful dissent in *Cobb* propounds similar suggestions in the hopes of limiting the scope of a warrant for electronic devices. 970 F.3d at 333 (Floyd, J., dissenting). There, an officer who had never searched a computer before obtained a warrant to search a computer for evidence of homicide. During his computer search, the officer discovered child pornography. Having seen this new, unrelated conduct, the officer sent the computer along for forensic analysis without obtaining a second warrant. *Id.*

This Court shares Judge Floyd’s reticence to permit unrestrained contours around searches of electronic media. What private-sector technology can collect and save has far

To the extent that Skinner contends that when the “place” to be searched is an electronic device, describing the manner of search or constraining it to items already known to law enforcement, the Fourth Circuit has now twice rejected that paradigm. In *Cobb*, the Fourth Circuit repeated *Williams*’ precedent “that so long as probable cause and particularity are met, executing officers are ‘impliedly authorized . . . to open each file on the computer to view its contents, at least cursorily, to determine whether the file [falls] within the scope of the warrant’s authorization’” because it relates to the designated crimes. *Id.* (quoting *Williams* 592 F3d at 521–22). While the private sector now stores layers of detailed information in the products they offer (and whose use have become ubiquitous), absent the creation of a tandem tool to unwind the information in a privacy-protecting manner, law enforcement is constrained to gather information in the manner these companies say that they can produce it.

The Fourth Circuit has stated, “the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents.” *Williams*, 592 F.3d at 523. As with a search of a file cabinet, conducting a search of computer files for evidence of criminal activity necessarily requires law enforcement to sort through vast amounts of information to find the particular evidence specified in the warrant. The Fourth Circuit in *Williams*, commenting on this difficulty, stated

[t]o conduct that [computer] search, the warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant’s authorization -i.e., whether it related to the designated Virginia crimes of making threats or computer harassment

---

outpaced that which any existing law anticipates, and it continues to do so at exponential rates. Absent curtailing regulation on the private-sector collection, it is difficult to weigh what the government should or should not be afforded access to while preserving due process and constitutional protections. As discussed in this Memorandum Opinion, the uncontroverted evidence showed that the Cellebrite technology used by the Government had no ability to dissect the data in the phones.

. . . . To be effective, such a search could not be limited to reviewing only the files' designation or labeling, because the designation or labeling of files on a computer can easily be manipulated to hide their substance. Surely, the owner of a computer, who is engaged in criminal conduct on that computer, will not label his [or her] files to indicate their criminality.

*Id.* at 522 (citations omitted).<sup>20</sup>

Here, not only the controlling law but the Gonzalez Affidavit and evidence presented in Court countermand the overbreadth concerns raised by Skinner. The cell phones are an instrumentality of the crime, the Gonzalez Affidavit explains how cell phones, including smart phones, function. The Affidavit also identifies Discord as an application designed for gaming communities to text, video, or talk over a chat channel. (Gonzalez Aff. ¶ 15(i).) Regarding search protocol, Gonzalez states that computer files on a cell phone's internal memory or SIM card, or their remnants, can be recovered months after they have been downloaded.<sup>21</sup> (*Id.* ¶ 25.)

The Gonzalez affidavit makes clear that a forensic analysis can show who has controlled the device and demonstrate the timing of file creation or chats by examining deleted files or

---

<sup>20</sup> The Second Circuit has explained in the context of computer searches:

it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes. Files and documents can easily be given misleading or coded names, and words that might be expected to occur in pertinent documents can be encrypted; even very simple codes can defeat a pre-planned word search.

*Ulbricht*, 858 F.3d at 102 (noting that a limited keyword search would not find items seized in the warrant there, which included a file discussing "aliases" and a folder named "mbsobzvkhwx4hmjt.").

<sup>21</sup> Gonzalez's explanation of the hurdles in searching computer information extends beyond current Fourth Circuit precedent. It clearly represents a best practice.

Some jurisdictions require the description of a protocol in order to approve an electronic search. *Ulbricht*, 858 F.3d at 102. If Congressional legislation cannot keep pace with developing technology, it seems—at least—that courts could demand more precise search protocol as technology allows us, over time, to pinpoint a less intrusive search to which the government would have to adapt. *Hill*, 459 F.3d at 979.

“cache” files (those viewed on the internet sometimes automatically downloaded in a temporary directory). (*Id.*) The Gonzalez Affidavit indicates that, depending on the volume of stored data, the dynamic review of the information necessary to draw an accurate conclusion, and the forensic tools necessary to evaluate a device’s particular configurations, could take weeks or months, and “would be impractical and invasive to attempt on-site.” (*Id.* ¶ 29(a).) *See Hill*, 459 F.3d at 974 (noting that the myriad and changing versions of Windows or Mac operating systems prevent on-site search when officers lack knowledge of which one the device employs uses, that on-site searches might corrupt the device or the evidence, and that files frequently are encoded).

Finally, the Gonzalez Affidavit also explains that while “it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators,” because reviewing the data in context, including whether counter-forensic programs exist, requires specialized knowledge about “how a computer behaves.” (*Id.* ¶ 28(d).) As demonstrated above, *Cobb* and *Williams* explicitly permit this type of search.

Thus, given the nature of the charged offenses, the ties between Skinner’s shopping and location history and the charged offenses, and the medium being searched, it cannot be said that the Cell Phone Warrant authorized an “exploratory rummaging in [Skinner’s] belongings.” *Dargan*, 738 F.3d at 647 (internal citation and quotations omitted). As the Fourth Circuit has found regarding the search of an electronic device capturing *all* data from a car after a collision for the limited purpose of assessing speed and other pre-crash data, “[n]o officer executing this warrant could have been mistaken as to the data he [or she] was authorized to obtain or the place where he [or she] could find it.” *Blakeney*, 949 F.3d at 864. No indication that any officer exceeded the scope of the warrants they executed exists on this record.



**c. The Gmail Warrants Were Valid Because They Identified the Items To Be Searched and Provided Probable Cause**

The Court also finds, given these facts and under binding law, the Gmail Warrants meet the requirements of the Fourth Amendment. As in his challenge to the Cell Phones Warrant, Skinner claims that the Gmail Warrants fail to particularly describe the items to be searched and seized and lacked probable cause for the items that were listed.

**i. The Gmail Warrants Were Sufficiently Particular**

The Gmail Warrants were sufficiently particular. To meet the particularity requirement, the warrant must “confine[] the executing [officers’] discretion by allowing them to seize only evidence of a particular crime.” *Cobb*, 970 F.3d at 328 (quoting *Fawole*, 785 F.2d at 1144). Because, like the Cell Phones Warrant, the Gmail Warrants confined “the items to be seized by their relation to designated crimes” and the description left “nothing to the discretion of the officer[s] executing the warrant,” *Williams*, 592 F.3d at 519, the Magistrate Judge had “a ‘substantial basis’ for concluding that probable cause existed.” *Abramski*, 706 F.3d at 314.

Like the Cell Phones Warrant, the Gmail Warrants authorized the seizure of files from Skinner’s Gmail Accounts that constituted “fruits, contraband, evidence and instrumentalities” of four specific federal crimes: Production of Child Pornography,<sup>22</sup> Distribution or Receipt of Child Pornography, Coercion and Enticement, and Kidnapping. (Gmail Warrant Attach. B 1.)

---

<sup>22</sup> The Weber Affidavit lists Production of Child Pornography, 18 U.S.C. § 2251(a), as one of the relevant statutory provisions. (Webber Aff. ¶ 7.) Attachment B of the Gmail Warrants omits this criminal statute but includes the other three previously listed criminal violations. (See Gmail Warrants, Attach B. 2.) This omission does not materially alter the effect of the Gmail Warrants because the Weber Affidavit included § 2251(a) as a relevant statutory provision. (Webber Aff. ¶ 7.) Furthermore, the other child pornography statute, 18 U.S.C. § 2252A(a)(2), which is listed in Attachment B, deals with largely the same subject matter as 18 U.S.C. § 2251(a) and criminalizes the Distribution of Receipt of Child Pornography. Therefore, any files discovered on Skinner’s Google Accounts relating to child pornography could be seized pursuant to that statute as well.

Like the Cell Phones Warrant, the Gmail Warrants further limited the executing officers' discretion by identifying certain types of records which law enforcement could search. The Gmail Warrant authorized the search of certain categories of records—similar to those in the Cell Phone Warrant—relating to “visual depictions of minors;” “any and all communications with other individuals about Victim 1;” and “any and all documents relating to [Skinner’s] plans to travel, or his actual travel, from New Zealand to the Richmond, Virginia area.” (*Id.*) The Gmail Warrants also identified categories of records specific to Gmail, such as authorizing the search and seizure of “other accounts with which [Skinner’s Account] may have shared Google Drive content, specifically video and/or picture content.” (*Id.* 2.) Like the Cell Phones Warrant, the Gmail Warrants were sufficiently particular, as they limited the materials to be searched by reference to four specific federal criminal statutes, and further limited the search by reference to specific categories of records. (*See* Gmail Warrant, Attach. B 1 (setting out the specific categories of records to be searched for and the related crimes).)

Here, law enforcement’s search of Skinner’s Gmail accounts for information relating to visual depictions of minors, communications involving V1, child erotica, and travel plans between New Zealand and Richmond, Virginia, relate to both the kidnapping and child pornography charges and are cabined by reference to the criminal statutes listed in the warrant. Because the Gmail Warrants limited the eleven itemized subjects to be searched to those identified federal offenses, the Court finds that they meet the particularity requirement.

**ii. The Gmail Warrants Were Not Overbroad**

Skinner protests that the Gmail Warrants are broader than the Cell Phones Warrant because they “authorized a wholesale seizure of the entire contents of the account, to be sifted by law enforcement.” (Mot. Suppress 3.) Skinner notes that the “extraction report was 1,316 pages



long and contained the video described in Count Seven of the superseding indictment,” but that the FBI “took no steps to partition off any part of the phone” and instead “downloaded and kept the entire contents of the phone.” (Skinner Supp. Br. Mot. Suppress. 3–4.)

This argument does not persuade. First, the Gmail Warrants were limited in time, and permitted only the seizure of items relating to the listed criminal violations occurring after December 25, 2017 until the date of the warrant. (Johnvlogchamber Gmail Warrant, Attach. B 2.) But uncontroverted evidence adduced at the hearing shows that the program used to extract the data, Cellebrite, could not separate data by date. (U.S. Resp. Def’s Supp. Br. 3, Ex. 1, ECF No. 103; *see also* Feb. 13, 2020 Hr’g Tr. 98.) While a time-limited search and return clearly are preferable, an initial time-limited search could not occur. Here, the scope of extraction could be limited by only extraction type (logical, system, or physical), or to specific data such as messages, contacts, call logs, media, application data, files, hidden files, and deleted data. (*Id.*) As courts have had to recognize, the nature of electronic evidence requires that filtering occur at the review level. This means that a cursory review of innocuous material may sometimes happen in order to establish what information is relevant. *Williams*, 592 F.3d at 519–20.

Indeed, this record shows that the FBI agent who executed the warrant sought legal advice before start, and utilized his standard “practice to review all parts of the search warrant to include the attachments in order to determine what he could and could not look for. [The FBI] specifically wanted to know what their limitations were when executing the search.” (Feb. 13, 2020 Hr’g Tr. 41–42.)<sup>23</sup>

---

<sup>23</sup> Skinner uses the return on the Gmail Warrants to suggest that the return demonstrates *per se* overbreadth. (Feb. 13, 2020 Hr’g Tr. 69–70.) Skinner correctly identifies, for instance, that Google’s collection of data resulted in a return encompassing 58,776 files, 7057 documents,

Second, Skinner’s reasoning fails to account for the complexities of searching online platforms. To be sure, the warrant instructed Google to produce broad swaths of information, such as “all emails associated with” Skinner’s account. (Johnvlogchamber Gmail Warrant, Attach. B 1.) But the Government, by the terms of the warrant, could only seize specific, limited information from those broad raw materials Google produced. That is, the Government could only seize evidence related to those same four specific criminal categories, and the eleven enumerated types of records produced after December 25, 2017 up until the time of the warrant. (*Id.*) (“[i]nformation to be seized by the government”). The purpose of this two-step process was to ensure that law enforcement, not Google, identified the records relevant to the criminal conduct at issue. As the Weber Affidavit notes:

[t]he provider [Google] is neither qualified nor trained to search the account information as would a law enforcement officer. Only a trained agent, familiar with the statutory violations and facts of the case, can determine what items should or should not be seized. For these reasons, the Affiant requests the provider disclose the records listed in Section I of Attachment B, for the account(s) listed in Attachment A.

(Weber Aff. ¶ 24.)<sup>24</sup>

So while Google provided the Government with large portions of Skinner’s account, the plain terms of the Gmail Warrants limited the extent it could search those documents and records in both time and scope. While the Gmail Warrants authorized investigators “to open and

---

37,450 emails, 3825 graphs, and 4750 multimedia files. (*Id.* 68–70.) Skinner notes that the FBI still has those downloads. (*Id.* 70.)

The Court observes that, on Exhibit 3, page 2, the return identifies file items and then lists “Evidence Groups, Ungrouped: 58,776.” (*Id.* 88.) The next category reports this “Checked Items: 9; Unchecked items, 58,767.” (*Id.*) The Court finds that this entry comports more with suggesting that the FBI limited its search in accordance with the warrant than it does with “deleted” items as initially suggested by Counsel for Skinner during the hearing. (*Id.*)

<sup>24</sup> Special Agent Weber also read this portion of the Weber Affidavit during the February 13, 2020 Evidentiary Hearing.

cursorily view” many files, the mere observation of unrelated files “did not involve an intrusion on [Skinner’s] protected privacy interests beyond that already authorized by the warrant, regardless of the officer’s subjective motivations.” *Williams*, 592 F.3d at 523; *Hill*, 459 F.3d at 978 (noting that a baggie containing a white powder during a drug-related search could be seized even if it were labeled “flour” or “talcum powder”). Like the Cell Phones Warrants, the Gmail Warrants survive this Fourth Amendment challenge regarding overbreadth.

**iii. The Gmail Warrants Were Based on Sufficient Probable Cause Despite Not Including Profile Evidence of Child Pornography Collectors**

---

Given the “great deference” accorded to the issuing judicial officer’s decision, *Abramski*, 706 F.3d at 318, the Gmail Warrants set forth facts forming a substantial basis for the Magistrate Judge’s determination of probable cause. As with the Cell Phones Warrant, the Gmail Warrants listed relevant criminal statutes that law enforcement suspected Skinner of violating. The Gmail Warrants then listed eleven categories of records to be searched for evidence of those violations.

The Weber Affidavit sets out facts similar to those contained in the Cell Phones Warrant, but adds information linking Skinner’s alleged criminal conduct to his Gmail accounts. Special Agent Weber avers that during her search of Skinner’s “Huawei mobile phone” she discovered a six-minute-long video in which [REDACTED]

[REDACTED] Based on the file path, Weber and FBI forensic analysts determined that “this child pornography video was downloaded . . . from the Google Drive for [one of Skinner’s accounts].” (*Id.* ¶ 40.) Furthermore, Weber avers that during her review of Skinner’s “Samsung mobile phone” she identified several emails on a different Skinner Gmail account which contained “the home address of V1.” (*Id.* ¶ 41.) On that same

account, she located several emails relating to Skinner's itinerary and tickets from New Zealand to Richmond, Virginia. (*Id.* ¶ 42.)

The Weber Affidavit thereby linked Skinner's Gmail Accounts to the offenses involving child pornography and kidnapping. Given this information, as well as the other information included in the Cell Phones Warrant regarding alleged child pornography and kidnapping offenses that would be found in Skinner's electronic accounts, the Magistrate Judge had a reasonable basis for concluding that additional pornographic images of V1 and information relating to the alleged attempted kidnapping could be found on the Gmail Accounts.

Skinner argues, however, that the Gmail Warrants omit a portion of the Cell Phones Warrant. As Skinner notes, unlike the Gonzalez Affidavit, the Weber Affidavit fails to include the "collector" profile of child pornographers. The United States admits that the "collector" profile was "inadvertently" omitted from the Gmail Warrants. (U.S. Resp. 9.) The Court finds this omission far from fatal to the Magistrate Judge's determination of probable cause.

The Court sees some tension between Skinner claiming harm from the *inclusion* of the collection profile in the Cell Phones Warrants while also decrying its absence in the Gmail Warrants. As stated above, no court has yet limited electronic searches for pornography to only those images known to be contraband. It would unduly burden law enforcement to search for only for a few pictures of one minor when law enforcement knows that the identity of the minor might not be immediately apparent based off the images it has already reviewed. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] To authorize law enforcement only to seize evidence of the production of child pornography involving V1 but not of other underage individuals would put reviewing officers in

an untenable position, where they would be forced to determine whether a lascivious sexual video or picture (1) involved a minor; and, (2) if it did, whether that minor was V1, before being authorized to seize that video. Such a reading of the Gmail Warrants would be at odds with the “commonsense and realistic approach” required in the Fourth Circuit. *Williams*, 592 F.3d at 519 (internal citations omitted). Fourth Circuit law does not require this.

The Gmail Warrants’ authorization for searching communications and videos involving “minors” did not lack probable cause where there existed substantial evidence that criminal production of child pornography could be found involving at least one minor. Regardless, even if the absence of the “collector” profile rendered the Magistrate Judge’s determination of probable cause deficient, the Gmail Warrants would be found valid under the good-faith exception.

**d. Even If the Warrants Were Lacking in Probable Cause, the Good-Faith Exception Would Apply Because Law Enforcement Reasonably Relied on the Magistrate Judge’s Probable Cause Determination**

The Cell Phones and Gmail Warrants were sufficiently particular and were based on probable cause. Even if they were not, the good-faith exception would apply to prevent the suppression of evidence in this case.

“Generally, evidence seized in violation of the Fourth Amendment is subject to suppression under the exclusionary rule, the overarching purpose of which is to deter future unlawful police conduct. *United States v. Andrews*, 577 F.3d 231, 235 (4th Cir. 2009) (internal quotation marks and citations omitted). The deterrence objective, however, “is not achieved through the suppression of evidence obtained by an officer acting with objective good faith within the scope of a search warrant issued by a magistrate.” *Id.* (internal quotation marks and citations omitted).

As a general rule, when a neutral magistrate has issued a warrant, the issuance “suffices to establish” that a law enforcement officer has “acted in good faith in conducting the search.” *United States v. Leon*, 468 U.S. 897, 922 (1984). Therefore, searches carried out pursuant to a warrant “rarely require any deep inquiry into reasonableness.” *Id.* For that reason, “[e]vidence obtained pursuant to a search warrant issued by a neutral magistrate does not need to be excluded if the officer’s reliance on the warrant was objectively reasonable.” *Id.* at 922–23.

An officer’s reliance on a warrant would not qualify as “objectively reasonable,” however, in the following four circumstances:

- First, where the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;
- Second, where the magistrate acted as a rubber stamp for the officers and so wholly abandoned’ his detached and neutral judicial role;
- Third, where a supporting affidavit is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and,
- Fourth, where a warrant is so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.

*United States v. Williams*, 548 F.3d 311, 317–18 (4th Cir. 2008) (internal quotation marks, alterations, and citations omitted). “In any of these four circumstances, then, the *Leon* good faith exception does not apply.” *Id.* When considering a motion to suppress the fruits of a novel investigative technique, courts decline to hold a warrant “facially deficient where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.” *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018).

Here, Skinner does not allege that the Magistrate Judge was “misled by information . . . that the affiant knew was false” or that the Magistrate Judges “wholly abandoned his judicial

role.” *Williams*, 548 F.3d at 317–18. The Court therefore turns to the final two prongs, noting at the outset that two experienced Magistrate Judges made separate yet similar findings that probable cause existed to search Skinner’s personal devices or emails for evidence of child pornography. These separate determinations by two Magistrate Judges weigh heavily against any argument that the Cell Phones and Gmail Warrants in this case “were so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable” or that the warrants were “facially deficient.”<sup>25</sup> *Id.*

The FBI also sought legal advice from the U.S. Attorney’s Office for the Eastern District of Virginia prior to securing the search warrants, further indicating that the agents acted in good faith in relying on the warrant. *Leon*, 468 U.S. at 902 (when evaluating good faith, observing officer had several deputy district attorneys review warrant application prior to submission); *United States v. Bynum*, 293 F.3d 192, 198 (4th Cir. 2002) (noting that officer’s decision to consult with prosecutor prior to applying for the search warrant provides additional evidence of objective good faith). On July 9, 2019, Special Agent Weber sent Assistant United States Attorney Brian Hood the first draft of the affidavit for the Cell Phone Warrant and had “multiple conversations [with Mr. Hood] regarding the ongoing investigation and the affidavit, draft of the affidavit.” (Feb. 13, 2020 Hr’g Tr. 36.) Taking the substantial investigatory information in the

---

<sup>25</sup> As previously discussed, the Cell Phones and Gmail Warrants at issue were based largely on several factors supporting the existence of probable cause: (1) V1’s minor status; (2) an independent review of V1’s cell phone and Discord chats with Skinner; (3) an interview with V1 where she confirmed that Skinner used Discord on his cell phone and computer; [REDACTED] (5) Skinner’s statements that he was trying to reach his thirteen year old girlfriend at the time of his capture; [REDACTED]

[REDACTED] The Gmail Warrants relied on the same information, but also included media seized during the execution of the Cell Phone Warrant, which Special Agent Weber determined, in her experience, to be child pornography. (Weber Aff. ¶¶ 39–40.)



warrants and the Government's legal review into account, a reasonable officer would believe probable cause existed to search the cell phones and Gmail accounts. Under these circumstances, the good-faith exception applies. *See Williams*, 548 F.3d at 317 (under the good faith exception, "evidence obtained pursuant to a search warrant issued by a neutral magistrate does not need to be excluded if the officer's reliance on the warrant was objectively reasonable") (internal quotation marks and citations omitted).

Nor can it be said that the three warrants were facially deficient in "failing to particularize the place to be searched or the things to be seized." *United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011). The warrants specifically identified the places to be searched—Skinner's two cell phones and two Gmail accounts. Furthermore, the warrants limited the searches to evidence of four federal crimes and ten or eleven categories of records in which officers believed evidence might be found. Considering these narrow categories and substantial limitations, a reasonable officer would not find the warrant facially unparticular.<sup>26</sup>

Like most searches carried out pursuant to a warrant, the case at bar does not "require any deep inquiry into reasonableness." *Leon*, 468 U.S. at 922. The warrants provided substantial evidence that violations of four federal statutes could be found on Skinner's cell phones and in Gmail accounts. Fourth Circuit precedent allows such searches. *See, e.g., Cobb*, 970 F.3d at

---

<sup>26</sup> On this point, Skinner cites *United States v. Marcus*, where a district court found officers failed to act in good faith in relying on a warrant. 807 F. Supp. 934, 937 (E.D.N.Y. 1992). But the warrant in *Marcus* authorized the search of all documents in a residence where there existed only probable cause to search a suitcase sent as a controlled delivery "primarily to provide a pretext for a patently invalid search warrant and the illegal search and seizure that followed." *Id.* Here, the warrants set out ample probable cause that there existed pornographic images of a child on Skinner's cell phones and Gmail accounts because the agents knew of many related files or chats. That is, the "suitcase" here was the Discord chats and pictures about which law enforcement had knowledge. Given the nature of the technology at issue, the warrants could hardly have been more specific about the extent of the property to be searched. *See Ulbricht*, 858 F.3d at 100 ("searches of computers may sometimes need to be as broad as searches of residences pursuant to warrants.").

323. Law enforcement established that evidence collected through investigation, including interviewing V1 who confirmed the presence of child pornography on the devices to be searched. Law enforcement then submitted the warrant applications to prosecutors for legal review, and neutral and detached Magistrate Judges subsequently approved them. While Skinner asks important questions about how to fairly search troves of electronic information, neither the courts nor Congress have provided a definitive answer to use as a measuring stick. On this record, the good-faith exception would apply to each warrant.

**B. The 29-Day Delay Between Seizing Skinner’s Cell Phones and Obtaining a Search Warrant Was Reasonable Given the Facts of this Case**

Skinner also contends that the twenty-nine-day delay between the seizure of his cell phones and the Magistrate Judge’s approval of the Cell Phones Warrant was unreasonable under the Fourth Amendment. The Court determines that given the facts of this case the delay was reasonable.

**1. Legal Standard: Reasonableness of Delay in Seeking Search Warrants**

“A seizure that is ‘lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests.’”<sup>27</sup> *United States v. Pratt*, 915 F.3d 266, 271 (4th Cir. 2019) (quoting *United States v. Jacobsen*, 466 U.S. 109, 124, (1984)). In determining whether the duration of the seizure was lawful, the court must “balance the government’s interest in the seizure against the individual’s possessory interest in the object seized.” *Pratt*, 915 F.3d at 271 (citations omitted). “A strong government interest can justify an extended seizure.” *Id.* Ultimately, the court “will uphold a temporary warrantless seizure if it

---

<sup>27</sup> “A seizure affects only the person’s possessory interests; a search affects a person’s privacy interests.” *Segura v. United States*, 468 U.S. 796, 806 (1984). Here, the Court focuses on Skinner’s possessory interest in his cell phones and the Government’s interest in the seizure.

was supported by probable cause, and was designed to prevent the loss of evidence while the police diligently obtained a warrant in a reasonable period of time.” *United States v. Burton*, 756 F. App’x 295, 299 (4th Cir. 2018) (internal quotation marks and citations omitted). The reasonableness of the seizure may vary due to “the nature and complexity of the investigation . . . the diversion of law enforcement to another case . . . [and] the quality of the warrant application and the amount of time . . . such a warrant would take to prepare.” *United States v. Laist*, 702 F.3d 608, 614 (11th Cir. 2012).

## **2. Facts Relating to the Government Seeking the Cell Phones Warrant**

On Friday, June 22, 2018, “Goochland County Sheriff’s Office responded to a 911 call in Goochland. And at that point they found the defendant, Mr. Skinner, in the front yard of a neighbor’s house with a gunshot wound to the neck.” (Feb. 13, 2020 Hr’g Tr. 10.)<sup>28</sup> Special Agent Weber was not on the scene. (*Id.*) The Goochland County Sheriff’s Office arrested Skinner, and “recovered two cell phones . . . a sweatshirt, a knife that was in an open position, pepper spray, a backpack which contained duct tape, along with several personal items to include clothing, travel documents, and Mr. Skinner’s passport.” (*Id.* 11–12.) The Goochland County Sheriff’s Office “took custody of the evidence” and transported Skinner to VCU Medical Center. (*Id.* 12–13.) Special Agent Weber stated that Skinner would not have been allowed to possess the cell phones during his stay at the hospital, which lasted from June 22, 2018 to July 22, 2018. (*Id.* 15.) Skinner did not indicate to Goochland County Sheriff’s Office Deputies “that he wanted his cell phones back” during his stay in the hospital. (*Id.*)

On Monday June 25, 2018, Agent Weber collected Skinner’s cell phones and “took them back to the FBI office, and . . . secured them in a locked container.” (*Id.* 19.) On June 26, 2018,

---

<sup>28</sup> In this section, the Court relates the facts as conveyed by Special Agent Weber, the lead FBI investigator in the Skinner case, at the February 13, 2020 Evidentiary Hearing.

the FBI opened its investigative file. (*Id.* 24.) On June 27, 2018, after conversations between the FBI, the Goochland County Sheriff's Office, the United States Attorney's Office ("USAO"), and the Goochland County Commonwealth's Attorney's Office, the USAO decided to accept the case for federal prosecution and opened a case file. (*Id.* 20–21.) In the five days between Skinner's arrest and the USAO's opening of the case, Goochland County Sheriff's Office did not seek a search warrant for the cell phones. (*Id.* 21.) At that time, no member of the Goochland County Sheriff's Office was a qualified Title 18 law enforcement officer able to serve as an affiant for a federal search warrant—a process that involves a background check and typically takes a "couple of months." (*Id.* 21–22.)

Following the USAO's opening of the case on June 27, 2020 and while Skinner remained hospitalized, Special Agent Weber took the following actions in relation to the investigation:

- On June 28, 2018, Special Agent Weber "reviewed portions of the minor victim's Discord account on her cellular phone" which was provided to her by the Goochland County Sheriff's Office on June 25, 2018. Later that day, Agent Weber met "with a forensic and adult – child and adult forensic interview by an FBI child and adult forensic interviewer" who conducted an interview of V1 that same day. (*Id.* 24.)
- On Friday, June 29, 2018, Special Agent Weber "finalized the evidence log for the four items collected on June 25th . . . [and] completed the foreign dissemination report for New Zealand authorities." (*Id.* 25.)
- On Tuesday, July 3, 2018, Special Agent Weber visited the "Walmart in Short Pump in order to review security footage which showed the defendant purchasing pepper spray, duct tape, and a knife." (*Id.* 26.)
- On Monday, July 9, 2018, Special Agent Weber provided "the first draft of the affidavit for the cell phone warrant to the [USAO]." (*Id.*)
- On July 12, 2018, Special Agent Weber conferred with the USAO in Richmond "regarding the best way to obtain evidence from New Zealand." (*Id.* 27.)
- On July 13, 2018, Special Agent Weber "returned to the aforementioned Walmart to obtain copies of the security footage that they hadn't been able to

provide a copy of on July 3, and . . . obtained additional information that day as well.” (*Id.*)

- On July 17, 2018, Special Agent Weber “conferred with the Department of Justice Office of International Affairs and New Zealand officials about the process for obtaining evidence from New Zealand.” (*Id.*)

During this time, Special Agent Weber was leading “approximately 27 pending cases,” while “approximately nine” of those cases involved crimes against children. (*Id.* 31.) Special Agent Weber also participated in other investigations, including: (1) on June 27, 2018, a search for a missing teenager in Dinwiddie, Virginia, (*id.* 30); (2) on July 2, 2018, a search at FCI Petersburg relating to an assault of an inmate by a correctional officer, (*id.* 31); and, (3) on July 3, 2018, an interview in Greenville County relating to a public corruption investigation, (*id.* 30). Additionally, on June 26, 2018, June 27, 2018, and July 6, 2018, Special Agent Weber acted as her squad supervisor, a position which required her to supervise and coordinate “the day-to-day functioning of the squad”—responsible for all child exploitation, public corruption, and civil rights investigations for the Richmond FBI Office. (*Id.* 32–33). During this time, Special Agent Weber’s supervisor was promoted, and she began to undertake his responsibilities and transition into an acting supervisor role. (*Id.*) From July 15 through July 20, 2018, Special Agent Weber attended Cyber Security training in Washington, D.C. (*Id.* 35).

Between the opening of the federal case on June 27, 2018 and July 20, 2018—the day then-Magistrate Judge Novak approved the Cell Phones Warrant—Special Agent Weber had “multiple conversations regarding the ongoing investigation and the affidavit” with Assistant United States Attorney Hood. (*Id.* 36.) Special Agent Weber also reported that after she sent

Attorney Hood a draft of the warrant application, she recalled that the USAO sent back a revised draft in which “there had been significant additional detail added.” (*Id.* 53.)

Special Agent Weber also had numerous conversations with the FBI legal attaché in New Zealand and other Department of Justice components about the international nature of the case. (*Id.* 28.) In Special Agent Weber’s words, the case demanded significant attention because

[t]his was the first case I had worked with an international aspect. I had not dealt with our legal attachés in this manner before. I had not dealt with [foreign dissemination reports] prior to this. And so I spent a lot of time coordinating with our [assistant legal attaché] determining what I could and could not produce, what New Zealand could and could not do or produce to us.

(*Id.*)

In mid-July, because Special Agent Weber knew that she “was going to be out of the office for a week [for training] and unable to be the affiant” for the Cell Phone Warrant, she requested that a coworker, Special Agent Melvin Gonzalez, serve as the affiant. (*Id.* 36–37.) On July 20, 2018, then-Magistrate Judge Novak signed the warrant authorizing the search of the cell phones seized from Skinner. Then-Magistrate Judge Novak signed the Cell Phone Warrant twenty-nine days after law enforcement officers seized the phones at the scene of Skinner’s arrest, twenty-five days after the FBI opened its investigation, twenty-four days after the USAO opened its case file, and two days before Skinner was released from the hospital and placed in custody.

**3. The 29-Day Delay Between Seizure of the Cell Phones and Approval of the Cell Phones Warrant Was Reasonable Considering the Complexity of the Case, the Timely Investigation of Officers, and the Deliberate Review Process**

The Court concludes that the twenty-nine-day delay between seizure of Skinner’s cell phones and the Magistrate Judge’s approval of the Cell Phone Warrant did not violate the Fourth Amendment given the Government’s strong interest in a continued seizure and the Government’s diligence in pursuing the investigation that involved working with a foreign country.



**a.     The Government Had a Strong Interest in the Seizure and Retention  
of Skinner's Cell Phone Given the Likelihood That Substantial  
Evidence of Federal Crimes Would Be Found**

---

Law enforcement had a substantial basis for retaining Skinner's cell phones because he was arrested after being shot while trying to illegally enter the home of a minor child with whom he had previously had a sexual online relationship.

Skinner was arrested after using substantial force to enter a home with an open switchblade, duct tape, and pepper spray on his person. Skinner initially explained to state law enforcement that he was attempting to reach his girlfriend, a minor. The day after the incident, the Goochland Sheriff's Department informed the FBI about a "child exploitation matter involving a 14-year old minor female" who had engaged in "sexual" communications with Skinner through an application called Discord. According to the Gonzalez Affidavit, law enforcement confirmed shortly after apprehending Skinner strong evidence suggested that the cell phones held evidence of a serious federal crime.

With this information, federal authorities possessed a substantial basis for concluding that Skinner had engaged in the production and dissemination of child pornography and that evidence of those offenses, among others, would be found on Skinner's cell phones. *See Pratt*, 915 F.3d at 271 ("A strong government interest can justify an extended seizure."). This information weighs heavily in favor of the Government's interest in maintaining custody of Skinner's cell phones.

Additionally, Skinner had a diminished possessory interest in the cell phones because he was detained and hospitalized following his arrest, the Cell Phones Warrant issued while he was in the hospital, and he remains in custody. *See United States v. Berroa*, 2021 WL 149254, at \*5 (D. Mass. Jan. 15, 2021) (in evaluating reasonableness of delay in obtaining a search warrant,



courts may consider whether a defendant has been in custody since arrest and has access to personal devices); *United States v. Brantley*, 2017 WL 5988833, at \*2 (N.D. Ga. Dec. 4, 2017) (“Brantley, having been arrested and detained, was not deprived of access to and use of the seized cellular telephones, because he was in custody, and he does not contend he was allowed possession of a cell phone while detained.”); *United States v. Kowalczyk*, 2012 WL 3201975, at \*23 (D. Or. Aug. 3, 2012) (“[S]ince Kowalczyk was in custody, there was no evidence that withholding access to his computers and other digital evidence was prejudicial; he had no serious possessory interest at stake.”). Special Agent Weber testified that Skinner would not have been allowed to possess the cell phones during his stay at the hospital, which lasted from June 22, 2018 to July 22, 2018. Furthermore, the record does not show that Skinner or anyone else requested the return of the cell phones, either during the twenty-nine-day delay in question or at any time prior to the February 13, 2020 Evidentiary Hearing. (*See, e.g.*, Feb. 13, 2020 Hr’g Tr. 15.) Skinner’s diminished possessory interest in the cell phones, when considered against the Government’s strong interest in the seizure, weighs in favor of the Government.

**b. The Government Diligently Pursued Its Investigation**

The duration of the twenty-nine-day period was not unreasonable considering that the case required contacting law enforcement authorities in New Zealand and the workload of the agents involved. The FBI took custody of the cell phones on Monday, June 25. (*Id.* 19.) The FBI opened its investigation on June 26, 2018, and the USAO opened its case file the next day on June 27, 2018. (U.S. Resp. 18, ECF No. 80.) That same day, the Special Agent in Charge coordinated with FBI personnel to establish contact with New Zealand authorities, but the next

day was “called to assist the FBI Evidence Response Team with the search for a missing 17-year-old in Dinwiddie, Virginia.” (U.S. Resp. 9; Feb. 13, 2020 Hr’g Tr. 30.)

On June 28, 2018, the following day, the FBI arranged for V1 to speak to the forensic interviewer and Special Agent Weber “reviewed portions of the minor victim’s Discord account on her cellular phone,” which was provided to her by the Goochland County Sherriff’s Office. (Feb. 13, 2020 Hr’g Tr. 24.) The Gonzalez Affidavit and the Cell Phones Warrant application relies in substantial part on V1’s testimony for its determination of probable cause. (*See* Gonzalez Aff. ¶¶ 32–40.) Throughout late June and early July of 2018, Special Agent Weber continued to collect evidence from New Zealand authorities, the Walmart store in Glen Allen, and other sources, all while consulting with the FBI’s legal attaché in New Zealand, “the Department of Justice Office of International Affairs and New Zealand officials about the process for obtaining evidence from New Zealand.” (Feb. 13, 2020 Hr’g Tr. 27.)

On July 9, 2018, four business days after the interview of V1,<sup>29</sup> Special Agent Weber provided “the first draft of the affidavit for the cell phone warrant to the [USAO],” (*id.* 26), and in the following days continued to take investigatory actions and coordinate with other law enforcement stakeholders, (*see id.* 27). On July 19, 2018, after consultation between the USAO and the FBI, the Government made an appointment with the Magistrate Judge. (U.S. Resp. 19.) On July 20, 2019, the Magistrate Judge approved the Cell Phones Warrant. (*Id.* 20.) Throughout this time, the Special Agent in charge had twenty-seven other open cases, and was called away for multiple days of training, assisted in other investigations, took on a supervisory role in her office, and eventually asked a fellow agent to serve as a substitute affiant for the Cell Phones

---

<sup>29</sup> June 28, 2018 fell on a Thursday. Because the July 4<sup>th</sup> holiday fell on the Wednesday of the next week, only five business days elapsed between June 28, 2018 and July 9, 2018.

Warrant. (*See* Feb. 13, 2020 Hr’g Tr. 30–35.) The FBI forensic examiner sought additional legal advice regarding the warrant. (*Id.* 41.)

The Government provides a convincing justification for obtaining the Cell Phones Warrant twenty-nine days after seizure. *Pratt*, 915 F.3d at 272. As the Government explains, this case required coordination not only with state law enforcement but with New Zealand law enforcement. The delay was due in part to the careful gathering of evidence while law enforcement sought legal advice from counsel throughout the process. The Cell Phones Warrant provided significant facts about the defendant and information gleaned from investigatory interviews with the child victim, rather than mere boilerplate. The agent in charge had competing caseloads, and at the time she was tasked with a supervisory role in the Richmond FBI Office. Finally, the agent in charge and her team were called off the case for at least two days to search for a missing teenager and assisted in numerous other pressing investigations during the time period between the seizure of the cell phones and the approval of the search warrant.

These facts set distinguish this case from *Pratt*. In that case, the FBI arrested Pratt for running a juvenile prostitution ring. During the arrest raid, a seventeen-year-old prostitute informed the FBI that she had texted nude photos to Pratt’s phone. Pratt confirmed, at the scene, that the nude pictures existed. “Pratt refused to consent to the seizure or disclose the phone’s passcode, and the FBI agents did not obtain a warrant for thirty-one-days. *Id.* at 270. Throughout this period, Pratt remained free from police custody. *See* Brief of Pratt, TLW-16-207, 2017 WL 6806325, at \*11 (Dec. 27, 2017). The government’s only justification for the “delay in obtaining a warrant was that Pratt committed crimes in both North Carolina and South Carolina and agents had to decide where to seek a warrant.” *Id.* at 272. The government

conceded, however, that the location of the magistrate judge issuing the warrant was immaterial to a future prosecution. *Id.* Balancing the Government's interest in seizing the phone against Pratt's possessory interest, the Court found that the 31-day delay was unreasonable and the evidence from the phone should have been suppressed. *Id.* at 272–73. Specifically, the Fourth Circuit reasoned that Pratt's possessory interest in the phone remained undiminished because he refused to consent to its seizure or voluntarily share its contents. *Id.* at 272. The government's excuse for its delay—confusion surrounding the appropriate jurisdiction for the warrant—was unavailing and did not outweigh Pratt's possessory interests. *Id.* at 272–73.

Skinner's case presents a materially different scenario. Here, although innocent until proven guilty, Skinner was detained and in the hospital during the relevant twenty-nine-day period and remains in custody. The FBI did not obtain access to Skinner's phones until three days after his arrest and did not open an investigation for another day after that. Furthermore, it was not until six-days after the phone's seizure that the FBI could interview V1 and establish much of the information later used in the affidavit in support of the search warrant. And the investigators in *Pratt* did not face the same difficulties as the agents in this case, who needed to coordinate their actions with other federal government officials and foreign governments concerning the gathering of evidence from a foreign country. In contrast to the delay in *Pratt* relating to only an immaterial prosecutorial decision, the United States has demonstrated the diligence of law enforcement in securing the Cell Phones warrant.<sup>30</sup>

Skinner's detention also meaningfully differentiates this case from those cited in his brief because he was not able to use his cell phones at the time they were in the possession of the

---

<sup>30</sup> Skinner's argument contesting the reasonableness of the seizure asks the Court to make several judgment calls that it is ill-suited to make. For example, Skinner states that

Government. For example, Skinner relies heavily on “*United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009), where the Eleventh Circuit suppressed evidence from a search of a cell phone because law enforcement officers had delayed obtaining a search warrant for twenty-one days.” (Reply Mot. Suppress 5, ECF No. 92). In *Mitchell*, an agent seized a computer but failed to obtain a search warrant for twenty-one days. 565 F.3d at 1351. The suspect in that case was not in custody and remained free to use computers even after his hard drive was seized. The agent explained that he left town for a lengthy training and did not think the warrant was urgent. *Id.* The Eleventh Circuit considered the seizure unreasonable because the agent could have applied for a warrant before he left or passed the case to someone else. *Id.* at 1351–52.

In contrast to the defendants in *Mitchell* and *Pratt*, Skinner initially detained and hospitalized for one month following his arrest, he remains in custody, and as a result he cannot access his cell phones. Law enforcement officers also worked diligently on Skinner’s case and provide adequate justification for the twenty-nine-day delay in this complex case involving

---

[t]he government’s timeline in this case includes references to a training and some other investigative activity, but *nothing particularly taxing* that would have prevented the case agent from involving another agent in the case earlier or tasking the associated local law enforcement officers who were working on the case with obtaining the warrant.

(Skinner Rep. 5–6, ECF No. 92 (emphasis added).) The Court declines to become the arbiter of the FBI’s investigative schedule, and the degree to which it is or is not “particularly taxing.” *Id.* Unlike *Pratt*, the government has identified many significant investigatory concerns, including the complexity of the case, other law enforcement priorities, the need for legal counsel in the crafting of the search warrant, and the need to gather additional evidentiary material.

Given these competing investigatory needs, the Court finds the delay reasonable. Law enforcement officials encounter investigations of high importance daily. Indeed, the FBI Agent responsible for this case had nine other open investigations involving crimes against children during the same time period. (Feb. 13, 2020 Hr’g Tr. 31.)

coordination with a foreign country. Given the record before the Court, the twenty-nine-day delay in obtaining the Cell Phones Warrant was reasonable.

**C. Speedy Trial Act and the COVID-19 Pandemic**

Clearly, this case has been pending for some time. But given Skinner's six pretrial motions, coupled with significant briefing on the complex factual and legal issues raised in this case on which the Court heard in-person arguments in two separate hearings during the global COVID-19 pandemic, the Court finds that no speedy trial violation has occurred.

On October 2, 2019, the Court arraigned Skinner on the Superseding Indictment, declared this case "complex," and found it in the interests of justice to continue the trial in this matter. (*See* Oct. 2, 2019 Order 1, ECF No. 63 (citing 18 U.S.C. §§ 3161(h)(7)(A) and (B)(ii) (allowing a district court to exclude time from the Speedy Trial calculation where a case is "unusual or so complex, due to the . . . existence of novel questions of fact or law, that it is unreasonable to expect adequate preparation for pretrial proceedings or for the trial itself within the time limits established by this section").)) At the time, the Parties were still engaged in gathering evidence from law enforcement in New Zealand. (*See, e.g.*, Not. Case Status, ECF No. 66.) On October 30, 2019, the Court held a Status Conference during which the Parties requested an additional extension to complete the discovery process. (ECF No. 65.) On December 2, 2019, the Court held a second Status Conference and established a briefing schedule. (*See* ECF Nos. 67–68.) On January 10, 2020, 100 days after Skinner's first appearance on the Superseding Indictment, Skinner filed six pretrial motions, including the Motion to Suppress addressed here.<sup>31</sup>

---

<sup>31</sup> As previously stated, with acknowledgment from both Parties that the March 18 oral argument could not occur, the Court continued the second hearing in this case after the COVID-19 pandemic took hold, pursuant to General Orders 2020-03, 2020-06, 2020-07, 2020-12, 2020-15, and 2020-16, and accounting for the Parties' schedules. (*See, e.g.*, ECF No. 109.)

Section 3161(h) automatically excludes the period of time that Skinner's six pretrial motions have been pending. 18 U.S.C. 3161(h)(1)(D) ("Any period of delay resulting from other proceedings concerning the defendant, including but not limited to—delay resulting from any pretrial motion, from the filing of the motion through the conclusion of the hearing on, or other prompt disposition of, such motion."); *see also Bloate v. United States*, 559 U.S. 196, 206 (2010) ("the provision communicates Congress' judgment that delay resulting from pretrial motions is automatically excludable, i.e., excludable without district court findings, only from the time a motion is filed through the hearing or disposition point"). Regardless, the Court has had to delay the hearings in this matter several times, both at the Parties' request and due to the ongoing COVID-19 pandemic. (*See* ECF Nos. 108–109.)

Upon review, the Court properly excluded the 100 days between Skinner's first appearance on October 2, 2019, and Skinner's filings on January 10, 2020. This matter has involved complex factual and legal questions, such as the Government's gathering evidence from New Zealand law enforcement to novel questions of law concerning this Court's subject matter jurisdiction and Skinner's due process rights. Considering these complexities, the Court reiterates its finding that this matter is "unusual or so complex, due to the . . . existence of novel questions of fact or law" and that the ends of justice are served by continuing a trial and such an action outweighs the best interest of the public and the defendant in a speedy trial. 18 U.S.C. §§ 3161(h)(7)(A) and (B)(ii).

The Supreme Court of the United States directed courts to consider the following four factors to determine whether a violation of the constitutional right to a speedy trial has occurred: "(1) the length of the delay; (2) the reason for the delay; (3) whether [petitioner] timely asserted his [or her] right; and, (4) whether delay prejudiced [petitioner's] case." *United States v.*



*Hopkins*, 310 F.3d 145, 150 (4th Cir. 2002) (citing *Barker v. Wingo*, 407 U.S. 514, 530 (1972)).

The duration of the delay, in addition to being a factor in this test, also constitutes a threshold requirement because the defendant must establish that the length of the delay is at least presumptively prejudicial. *See Doggett v. United States*, 505 U.S. 647, 651–52 (1992). For a petitioner to prevail on a Speedy Trial Act challenge, the four factors must, on balance, weigh in his or her favor. *See United States v. Thomas*, 55 F.3d 144, 148 (4th Cir. 1995).

Considering the first factor, the length of the delay, the Court finds seventeen months from the superseding indictment in October 2019 to the issuance of this opinion in March 2021 presumptively prejudicial. The Supreme Court has suggested that a delay approaching one year is presumptively prejudicial. *Doggett*, 505 U.S. at 652 n.1. In addition, the Fourth Circuit has held that as a “general rule,” a “postaccusation delay as short as eight months may qualify as presumptively prejudicial in cases of limited complexity.” *United States v. Burgess*, 684 F.3d 445, 452 (4th Cir. 2012); *but see Hopkins*, 310 F.3d at 150 (concluding two-year delay before trial “was not uncommonly long” where superseding indictment involved, and defendant filed seven pretrial motions during that period).

The first factor weighs in favor of Skinner because the delay in this case is presumptively prejudicial. Skinner has been waiting more than one year for resolution on his six pretrial motions. However, unlike *Woolfolk*, which involved only a single defendant and one count, this case involves eleven counts and six pretrial motions implicating unique questions of fact and law. *See United States v. Woolfolk*, 399 F.3d 590, 598 (4th Cir. 2005) (“[G]iven the fact that Woolfolk’s case involves little complexity, we see no reason to deviate from th[e] general rule [that an eight-month delay is presumptively prejudicial] here.”). The Parties agreed that it

constitutes a complex case requiring delays they themselves sometimes sought. Nonetheless, the delay at bar raises a presumption of prejudice.

The Court must next determine whether the remaining factors favor Skinner. Looking to the second factor, the reason for the delay, the Court finds that this factor weighs against Skinner. The delay resulted from the Parties' need to gather evidence across international borders, both Parties' requests for continuances, Skinner's six pretrial Motions and substantial associated briefing, two evidentiary hearings, and the unavoidable complications associated with the COVID-19 pandemic. *See United States v. Pair*, No. 3:20cr3, 2021 WL 772235 (E.D. Va. Feb. 26, 2021) ("Both the COVID-19 pandemic and defense counsel's September 2020 motion are valid reasons for delay that weigh in favor of a finding that the Sixth Amendment right here at issue has not been violated."); *Turner v. Watson*, No. 3:11cv757, 2012 WL 3985627, at \*12 (E.D. Va. Sept. 11, 2012) (finding government should not be faulted for delay where defendant consented or otherwise contributed to need for continuance). Notably, the Eastern District of Virginia suspended criminal jury trials for much of 2020 and during the first two months of 2021, meaning that Skinner could not have faced a criminal jury trial in any event. *See Pair*, 2021 WL 772235, (explaining that "between March 16, 2020 and September 13, 2020, the Court suspended jury trials in the Eastern District of Virginia because of the COVID-19 pandemic."); *see also* Gen. Order 2020-22 (Case No. 2:20mc007, ECF No. 23) (Chief Judge Davis, observing the nationwide spike in COVID-19 cases and hospitalizations, suspending all criminal jury trials in the Eastern District of Virginia from November 19, 2020 until January 18, 2021); Gen. Order 2021-01 (Case No. 2:20mc007, ECF No. 26 (Chief Judge Davis further extending the suspension of all criminal jury trials until February 28, 2021)). As a result, this second factor weighs against Skinner.

Turning to the third factor, Skinner has not asserted his right to a speedy trial. Rather, he has requested several of the extensions that have delayed this matter. A defendant's timely and vigorous assertion of his or her speedy trial right can evince an intolerable delay, improper reasons for delay, or personal prejudice to the defendant (which can be hard to measure by other means). *United States v. Hall*, 551 F.3d 257, 271 (4th Cir. 2009) (directing courts to consider "the timeliness and vigor of the assertion"). For this reason, this factor "is entitled to strong evidentiary weight in determining whether the defendant is being deprived of the right." *Barker*, 407 U.S. at 531–32. The Supreme Court has emphasized that "failure to assert the right will make it difficult for a defendant to prove that he was denied a speedy trial." *Id.* at 532. Here, much of the delay is attributable to the COVID-19 pandemic and the pretrial motions that Skinner filed. Additionally, Skinner has not asserted his right to a speedy trial. *Hopkins*, 310 F.3d at 150. As a result, this factor weighs against Skinner.

Turning to the fourth factor, the delay has not prejudiced Skinner because, as detailed above, this Court has not been able to hold criminal jury trials during most of the COVID-19 pandemic that took hold in March 2020, roughly two weeks after the February 13, 2020 Evidentiary Hearing and while the Parties' filed supplemental cross-briefs on the instant Motion to Suppress. The Parties recognized that oral argument had to be delayed and sought a continued hearing. Prejudice must be considered "in the light of the interests of defendants which the speedy trial right was designed to protect," namely: "(i) to prevent oppressive pretrial incarceration; (ii) to minimize anxiety and concern of the accused; and (iii) to limit the possibility that the defense will be impaired." *Barker*, 407 U.S. at 532. The Supreme Court has counseled that the last interest is the "most serious . . . because the inability of a defendant adequately to prepare his case skews the fairness of the entire system." *Id.* In this case, Skinner

has faced oppressive pretrial incarceration and heightened anxiety due to the COVID-19 pandemic and the spread of the virus in prisons and jail. However, Skinner does not assert any impairment of his defense. He does not allege that any evidence was damaged or lost, that any witnesses could not be found, or that his case was harmed in any manner by the delay. *Hopkins*, 310 F.3d at 150. Indeed, it is the vigor of Skinner's sometimes evolving defense that has required a detailed examination of the novel issues he raises. Without a showing of prejudice, this factor weighs against Skinner.

The delays in this case are not the result of an improper Government purpose or of Government negligence. The Government pursued its prosecution with reasonable diligence, but delays occurred for valid reasons outside the control of either party. As a result, the Court concludes that the speedy trial factors do not weigh in favor of Skinner, despite the length of time that has passed since the superseding indictment and the issuance of this Memorandum Opinion. Under these circumstances and on this record, Skinner's Sixth Amendment right to a speedy trial has not been violated.

### III. Conclusion

For the foregoing reasons, the Court will deny the Motion to Suppress. (ECF No. 70.)  
An appropriate Order shall issue.

  
M. Hannah Lauck  
United States District Judge

Date: 3-10-21  
Richmond, Virginia